ОРГАНИЗАЦИЯ СОТРУДНИЧЕСТВА ЖЕЛЕЗНЫХ ДОРОГ (ОСЖД)

II издание

Разработано экспертами ОАО «РЖД» в 2018 году.

Согласовано Совещанием экспертов Постоянной рабочей группы по кодированию и информатике 11-13 сентября 2018 г., город Штурово.

Утверждено Итоговым совещанием Постоянной рабочей группы по кодированию и информатике 13-15 ноября 2018 г., город Варшава.

Дата вступления в силу: 15 ноября 2018 года.

Теряет силу: I издание от 20 ноября 2014 года

Р 941-4

Описание типовых технических спецификаций трансграничного взаимодействия «Инфраструктур открытых ключей» железных дорог – стран ОСЖД

Оглавление

Перечень принятых сокращений и обозначений.

АС	–	Автоматизированная система
АСОУП	–	Автоматизированная система оперативного управления перевозками
БЧ	–	Государственное объединение «Белорусская железная дорога»
ДТС	–	Доверенная третья сторона
ДУЦ	–	Доверенный удостоверяющий центр
ЕК	–	Европейская Комиссия
ИОК (PKI)	–	Инфраструктура открытых ключей
КЖД	–	Калининградская железная дорога – филиал ОАО "РЖД"
ЛГ	–	Акционерное общество «Литовские железные дороги»
ЛДЗ	-	ГАО «Latvijas dzelzceļš»
АО ЭВР	-	АО Эстонская железная дорога
АО «УБЖД»	-	Акционерное общество «УБЖД»
КТЖ, АО «НК «КТЖ»		Акционерное общество «Национальная компания «Казакстан темір жолы»
ОАО «РЖД»	–	Открытое акционерное общество «Российские железные дороги»
ПАК	–	Программно-аппаратный комплекс
СКЗИ	–	Средства криптографической защиты информации
СКПЭП	–	Сертификат ключа проверки электронной подписи
СОК	–	Сертификат открытого ключа
СПД	–	Сеть Передачи Данных
СЭДО	–	Система электронного документооборота
УЗ	–	Укрзализныця
УЦ	–	Удостоверяющий центр
ЭОД	–	Электронный обмен документами
ЭД	–	Электронный документ
(К)ЭП	–	(Квалифицированная) Электронная подпись
ЭЦП	–	Электронная цифровая подпись

Термины и определения

EDI	–	Electronic Data Interchange – электронный обмен данными
EDI-система	–	Система электронного обмена данными между иностранными железными дорогами
HSM	–	hardware security module – устройство для генерации и защищенного хранения ключевой информации
OCSP	–	Online Certificate Status Protocol – протокол для определения статуса СОК
RFC 3029	–	протокол «подтверждения подлинности электронного документа, подписанного ЭЦП»
RSA	–	криптографический алгоритм с открытым ключом
TLS	–	Transport Layer Security – криптографический протокол, обеспечивающий защищённую передачу данных между узлами в сети Интернет

TSP	–	Time-Stamp Protocol, протокол службы штампов времени
UN/EDIFACT	-	United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport (Правила ООН электронного обмена документами для государственного управления, торговли и транспорта)
VSD	–	Validation of Digitally Signed Document – Проверка действительности КЭП/ЭЦП на конкретный момент времени на электронном документе
XML	–	eXtensible Markup Language — расширяемый язык разметки
Адресат ЭД	–	Лицо, которое, согласно намерению Составителя ЭД, должно получить конкретный ЭД, подписанный ЭП/ЭЦП.
Инфраструктура открытых ключей	–	Организационно-техническая структура, предназначенная для применения средств ЭП/ЭЦП, идентификации лица, вырабатывающего ЭП/ЭЦП и подписывающего ЭД, подтверждения целостности и подлинности ЭД с помощью средств ЭП/ЭЦП в соответствии с законодательством Сторон.
Квалифицированная электронная подпись	–	Электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам: 1) ключ проверки электронной подписи указан в квалифицированном сертификате; 2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с действующим законодательством.
Ключ проверки электронной подписи (открытый ключ)	–	Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.
Ключ электронной подписи (закрытый ключ)	–	Уникальная последовательность символов, предназначенная для создания электронной подписи.
Неквалифицированная электронная подпись	–	Электронная подпись, которая: 1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи; 2) позволяет определить лицо, подписавшее электронный документ; 3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания; 4) создается с использованием средств электронной

		подписи.
Составитель ЭД	–	Лицо, которое или от имени которого ЭД подготовлен и подписан ЭП/ЭЦП в порядке, соответствующем законодательству государства, субъектом правового пространства которого является лицо.
Средства ЭП	–	Шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.
Электронный документ	–	Формализованная запись информации в электронном виде, заверенная ЭП/ЭЦП, соответствующая требованиям законодательства государства, субъектом правового пространства которого является Составитель ЭД.
Электронная подпись	–	Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.
Электронная цифровая подпись	–	Последовательность символов, являющихся реквизитом ЭД, предназначенных для подтверждения его целостности и подлинности и/или для идентификации лица, подписывающего ЭД, в соответствии с законодательством государства, субъектом правового пространства которого является Сторона.

1. Общие положения

В условиях глобализации экономики, создания крупных транснациональных корпораций и интеграции транспорта ряда государств в мировую экономику происходит интенсивный процесс формирования транспортных осей, обеспечивающих ускоренное продвижение крупных товарорматериальных и пассажирских потоков между странами. При этом новые экономические условия глобальной торговли и более жесткие требования к контролю качества и стоимости требуют создания новой системы регулирования и управления железнодорожным комплексом.

Для успешного развития железнодорожного транспорта, повышения его конкурентоспособности и привлекательности для инвесторов необходимо рациональное снижение издержек и повышение эффективности.

Внедрение юридически значимых электронных документов в международные перевозки создает правовые, организационные и технологические предпосылки для ускорения оборота товаров, денег и услуг, позволяет оптимизировать перевозки, существенно сократить затраты на их планирование и обеспечение.

Возможность применения электронного перевозочного документа предусмотрена параграфом 10 статьи 6 и параграфом 14 статьи 7 Соглашения о международном железнодорожном грузовом сообщении.

Информационное сопровождение грузовых перевозок в системах железнодорожных администраций осуществляется на основании соглашений об ЭОД в международном стандарте UN/EDIFACT по факту приема груза к перевозке с последующей передачей информации на приграничные станции для предварительного информирования и оформления документов по сетям передачи данных «Инфосеть-21», HERMES и сети Интернет.

Для обеспечения авторства электронных документов (ЭД), обеспечения их целостности и юридической значимости используются технологии электронной подписи (ЭП).

Целью применения юридически значимого ЭОД является обеспечение эффективной организации международного железнодорожного груз перевозочного процесса с использованием информационно – телекоммуникационных технологий.

Основными задачами при практической реализации юридически значимого ЭОД являются:

- разработка механизма признания юридического значения подписанного ЭП документа и обеспечения доверия сертификатам, изданным в разных правовых полях сторон;
- организация взаимодействия специальных программных и аппаратных средств сторон, т.к. субъекты информационного обмена могут находиться в правовых полях, определяющих взаимоисключаемость легитимно используемых криптографических алгоритмов;
- создание технических условий для передачи, обработки и проверки электронных документов, подписанных ЭП.

Для решения перечисленных проблем требуются надежные элементы доверия для достижения адекватных уровней защищенности информационного взаимодействия и обеспечения юридической значимости электронных документов. Эти предполагаемые элементы доверия между участниками информационного взаимодействия в недостаточной степени обеспечиваются существующими

информационными системами и, как правило, требуют участия «доверенной третьей стороны» (ДТС), чтобы способствовать надежному обмену информацией.

Сервисы ДТС описаны в международных рекомендациях ITU-T X.842 «Информационная технология – методы безопасности – Руководящие принципы для использования и управления услугами доверенной третьей стороны». Основной функцией ДТС является проверка ЭП, сформированной в рамках иностранного правового поля и криптографических стандартов и признание ее легитимности в соответствии с законодательством стороны-получателя ЭД.

Участники трансграничного взаимодействия (ЖД Администрации) для организации доверенного обмена электронными документами должны подключиться (или обеспечить самостоятельное подключение) к инфраструктуре доверия (точки доступа) – рис.1.

Точки доступа могут быть организованы как на базе подключаемой ЖД Администрации в соответствии с требованиями, излагаемыми в данной памятке, так и с привлечением независимых участников рынка (поставщиков доверенных услуг). Точки доступа обеспечивают организацию доверительных отношений с другими точками доступа, к которым в свою очередь подключены другие ЖД Администрации. Точка доступа, к которой подключается ЖД Администрация, должна быть локальной компанией, работающей в одном правовом поле с подключаемой ЖД Администрацией.

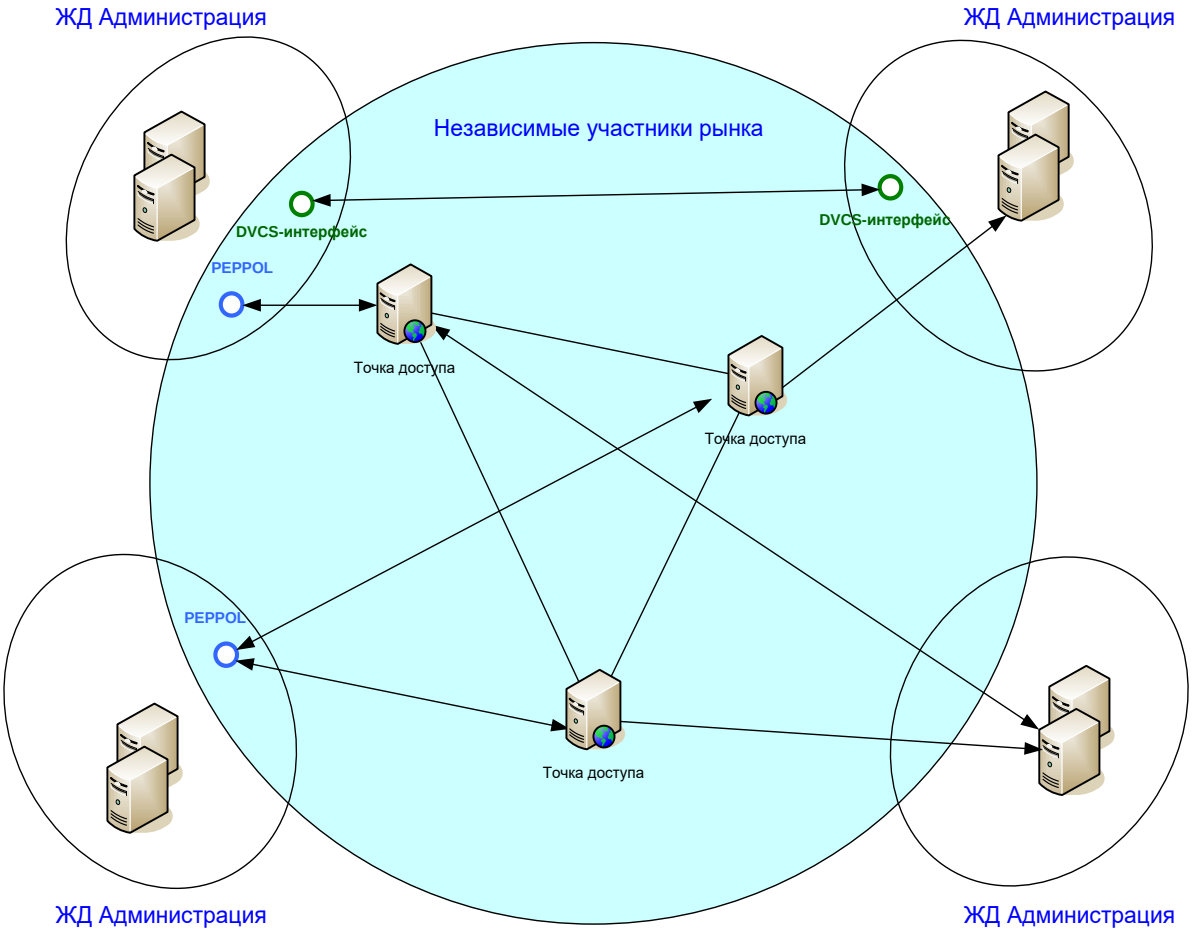


Рис 1. Взаимодействие инфраструктур открытых ключей

2. Описание технических спецификаций

2.1. ITU-T X.842 «Information technology-Security techniques. Guidelines for the use and management of trusted third party services» [1];

«Информационные технологии – Методы защиты – Руководящие указания по применению и управлению службами доверенной третьей стороны».

Рекомендации включают указания по применению и управлению службами доверенной третьей стороны (ДТС), чёткое определение выполняемых обязанностей и предоставляемых услуг, их описание и назначение, а также роль и ответственность третьей стороны и сторон, пользующихся её услугами. Документ предназначен, прежде всего, для системных администраторов, разработчиков, операторов ДТС и пользователей их услуг для выбора и эксплуатации необходимых сервисов ДТС.

В рекомендациях определены основные категории служб третьей стороны, в том числе фиксация времени, неотвергаемость, управление ключами и сертификатами, а также службы электронного нотариата.

Основные сервисы ДТС, представляемые в соответствии с международными рекомендациями X.842:

1. Проверки подлинности и действительности данных (по RFC 3029. Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (DVCS).
2. Управления сертификатами.
3. Проверки статуса сертификатов (по RFC 2560. Online Certificate Status Protocol - OCSP).
4. Выработки штампа времени (по RFC 3161. Time-Stamp Protocol).
5. Идентификации и аутентификации.
6. Электронного нотариата.
7. Контроля доступа.
8. Электронного архива.
9. Неотказуемости.
10. Каталогов.
11. Персонализации.
12. Управления ключами.
13. Служба трансляции.
14. Восстановления.
15. Управления оповещениями об инцидентах.

В соответствии с X.842 таких сервисов более 30.

2.2. PKCS #1 «RSA Cryptography Standard», v2.1 [2];

Public Key Cryptography Standards (Стандарты криптографии с открытым ключом) - спецификации, выработанные RSA Laboratories в сотрудничестве с разработчиками систем безопасности всего мира с целью разработки криптографии с открытым ключом.

Стандарт PKCS #1 описывает базовые принципы работы с открытыми ключами, основанными на алгоритме RSA (Rivest, Shamir, Adleman).

2.3. RFC 2560:1999, RFC 6960 «Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP» [3];

Online Certificate Status Protocol – протокол получения статуса сертификата в реальном времени. Применяется для предоставления пользователям УЦ актуальной информации о статусах сертификатов ключей подписи. По протоколу OCSP можно получить информацию об изменении статуса цифрового сертификата в реальном времени.

OCSP предоставляет сервис определения статуса сертификатов без обращения к спискам отозванных сертификатов со стороны клиентского программного обеспечения. Использование OCSP позволяет минимизировать накладные расходы для прикладных процедур, в которых по логике работы должна осуществляется проверка статуса сертификата клиентским программным обеспечением.

Протокол OCSP работает по принципу «запрос-ответ». OCSP-клиент генерирует OCSP-запрос и отправляет его на сервер. OCSP-сервер получает этот запрос, проверяет статус сертификата, генерирует OCSP-ответ и отсылает его клиенту.

Впервые был опубликован в RFC 2560 в 1999 г., последняя версия стандарта – RFC 6960, вышедшая в июне 2013 г. [4]

2.4. RFC 2315 «PKCS #7: Cryptographic Message Syntax Version 1.5» [5] ;
RFC 2630, RFC 5652 «Cryptographic Message Syntax» (CMS) [6] .

Cryptographic Message Syntax - Синтаксис криптографических сообщений. Описывает структуру криптографических сообщений, включающих в себя защищенные данные вместе со сведениями, необходимыми для их корректного открытия или использования. К таким сведениям относятся, например, защищенные данные, информация об алгоритме хеширования и подписи, времени подписи, сертификате открытого ключа, цепочке сертификации и т.д.

Стандарт CMS кроме электронной подписи поддерживает операции шифрования, хеширования и вычисления имитовставки, в том числе и по российским алгоритмам (RFC 4490), а также множественную инкапсуляцию (сообщение формата CMS может лежать внутри другого CMS сообщения).

CMS впервые был опубликован в качестве рекомендаций RFC 2315 «PKCS #7: Cryptographic Message Syntax Version 1.5» в марте 1998 г. Спустя еще несколько версий RFC (в том числе, RFC 2630) в сентябре 2009 года был принят RFC 5652 «Cryptographic Message Syntax (CMS)» [7], который является действующим стандартом на данный момент.

2.5. RFC 2510 [8], RFC 4210 «Internet X.509 Public Key Infrastructure. Certificate Management Protocols» (CMP) [9];

Certificate Management Protocol - протокол управления сертификатами, который используется для запросов на доступ и обработку сертификатов X.509. Определяет операции с сертификатами X.509, такие, как отправка запроса на подписание, получение подписанного сертификата и другие, а также несколько коммуникационных методов (таких, как HTTPS), которые могут быть использованы для транспортировки запросов сертификата по сети.

Последняя версия протокола описана в RFC 6712 [10].

2.6. RFC 5246 «The Transport Layer Security (TLS) Protocol», v1.2 [11];

Transport Layer Security (безопасность транспортного уровня)- криптографический протокол, обеспечивающий защищённую передачу данных между

узлами в сети Интернет. TLS использует асимметричную криптографию для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

Целью протокола TLS является обеспечение конфиденциальности и целостности данных при коммуникации двух приложений. Протокол имеет два уровня: протокол записей TLS и протокол диалога TLS.

Протокол записей TLS используется для инкапсуляции различных протоколов высокого уровня. Один из таких инкапсулируемых объектов, протокол диалога TLS, позволяет серверу и клиенту аутентифицировать друг друга и согласовать алгоритм шифрования и криптографические ключи до того как приложение передаст или примет первый байт информации. Протокол диалога TLS обеспечивает безопасное соединение, которое имеет три базовых свойства:

- Идентичность партнеров может быть выяснена с использованием асимметричной криптографии (напр., RSA, DSS и т.д.). Эта аутентификация может быть сделана опционной, но она необходима, по крайней мере, для одного из партнеров.
- Выявление общего секретного кода является безопасным: этот секретный код недоступен злоумышленнику, даже если он ухитрится подключиться к соединению.
- Диалог надежен: атакующий не может модифицировать обсуждаемое соединение, без того чтобы быть обнаруженным партнерами обмена.

2.7. RFC 4634 «US Secure Hash Algorithms» (SHA and HMAC-SHA) [12];

Secure Hash Algorithm - алгоритм стойкого хеширования. Хешированием называется преобразование исходного информационного массива произвольной длины в битовую строку фиксированной длины.

Алгоритм реализует хеш-функцию, построенную на идее функции сжатия. Входами функции сжатия являются, блок сообщения длиной 512 бит и выход предыдущего блока сообщения. Выход представляет собой значение всех хеш-блоков до этого момента. Хеш-значением всего сообщения является выход последнего блока.

HMAC (hash-based message authentication code*)* - хеш-код аутентификации сообщений. Механизмы, которые предоставляют проверки целостности на основе секретного ключа, обычно называют кодом аутентичности сообщения (MAC). Как правило, MAC используется между двумя сторонами, которые разделяют секретный ключ для проверки подлинности информации, передаваемой между этими сторонами. Этот стандарт определяет MAC. Механизм, который использует криптографические хеш-функции в сочетании с секретным ключом, называется HMAC.

2.8. RFC 5280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile» [13].

Certificate Revocation Lists (списки отзыва сертификатов) - — метод, с помощью которого сертификаты могут быть признаны недействительными до наступления даты, указанной в поле NotAfter сертификата. Обычно CRL выпускаются тем же УЦ, который выпустил и сам сертификат. CRL могут быть получены различными методами, например, посредством LDAP, HTTP или FTP. Формат CRL (в частности CRLv2, текущая версия) определён в RFC 5280, а затем обновлён в RFC 6818 [14].

3. Интерфейсы взаимодействия «инфраструктур открытых ключей», базирующиеся на спецификациях:

3.1. RFC 3029 «Internet X.509 Public Key Infrastructure. Data Validation and Certification Server Protocols» [15].

На базе данной спецификации реализовывается разовая или абонентская услуга по проверке и сертификации информации, проверки сертификатов и выработке квитанции, содержащих штамп времени (необязательная опция).

Полный набор сервисов DVCS:

1. Подтверждение факта наличия данных;
2. Подтверждение факта заявления о наличии данных;
3. Проверка подлинности ЭД;
4. проверка действительности СОК.

Результатом выполнения той или иной функции служит DVC квитанция, образованная службой ДТС.

3.2. OASIS DSS (OASIS Digital Signature Service)

Определяет XML-интерфейс для работы с цифровыми подписями для Web-сервисов и других приложений.

Схема реализации спецификации представлена в [16].

3.3. XKMS v2.0 (XML Key Management Specification)

Спецификации данного стандарта определяют технологию использования открытых ключей для обеспечения информационной безопасности XML-ресурсов. В частности, определяется протокол для распространения и регистрации открытых ключей, совместимый со стандартами консорциума W3C цифровой подписи XML Digital Signature и кодирования XML-ресурсов XML Encoding. Спецификации XKMS представляют два сервиса: XML Key Information Service и XML Key Registration.

XML Key Information Service Specification (X-KISS) - протокол для поддержки делегирования от приложения к серверу обработки информации ключа, ассоциированной с XML signature, XML encryption, или иного использования элемента XML Signature <ds:Key Info>.

XML Key Registration Service Specification (X-KRSS) - протокол для поддержки регистрации пары ключей владельцем пары, с целью впоследствии использовать пару ключей совместно с XKISS или PKI, таким как X.509 PKIX.

Основная цель применения спецификаций XKMS - переложить всю сложность реализации традиционного PKI с клиента на внешнюю службу.

Описание реализации стандарта XKMS представлено в [17].

3.4. Рекомендации Европейского института телекоммуникационных систем «Предоставление списка доверенных поставщиков услуг» ETSI TS 102 231 «Electronic Signatures and Infrastructures (ESI). v3.1.2 Provision of harmonized Trust-service status information», Annex B (normative): Implementation in XML

Предоставление списка доверенных поставщиков услуг (Trusted Service Status List). Задает формат доверенных списков (TSL-списки) аккредитованных УЦ.

Список может содержать не только сертификаты уполномоченных лиц аккредитованных УЦ, а так же включать в себя описания и ссылки на другие сервисы, предоставляемые аккредитованными УЦ, к которым относятся сервисы штампов времени (TSP), сервисы онлайновой проверки статусов сертификатов (OCSP) и др.

Применение TSL-списков должно оказать помощь пользователю при ответе на вопросы:

- предоставляет или предоставлял ли УЦ защищенную услугу;
- соответствует или соответствовало ли ее предоставление критериям схемы на момент оказания услуги или на момент совершения транзакции, основанной на продуктах услуги.

Описание организации TSL-списков представлено в [18].

4. Требования к программному обеспечению взаимного признания электронных подписей при реализации трансграничного информационного взаимодействия

4.1. Общие требования

4.1.1. Точка доступа ДТС должна предоставлять соответствующий схеме применения набор Web-служб, обеспечивающих функционирование комплексов третьей доверенной стороны: проверку электронной подписи и/или проверку сертификатов подписи.

4.1.2. Должна быть обеспечена возможность проверки ЭП в соответствии с одной следующих международных рекомендаций (в зависимости от схемы применения):

- RFC 3029 «Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols»: Validation of Digitally Signed Documents (DVCS);
- Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0 OASIS Standard (OASIS DSS).

4.1.3. Должна быть обеспечена (в зависимости от схемы применения) возможность проверки сертификата подписи в соответствии с рекомендациями W3C: XML Key Management Specification (XKMS 2.0).

4.1.4. Должен быть реализован список статусов доверенных сервисов и Удостоверяющих центров в соответствии с ETSI TS 102 231.

4.1.5. Точка доступа ДТС должна содержать в своем составе одну или несколько следующих программных компонент (в зависимости от схемы применения):

4.1.5.1. DVCS сервер.

4.1.5.2. DSS сервер.

4.1.5.3. XKMS сервер.

4.1.5.4. Программные модули генерации и работы со списком статусов доверенных сервисов (библиотека TSL).

4.1.5.5. DVCS клиент.

4.1.5.6. DSS клиент.

4.1.5.7. XKMS клиент.

4.1.6. Программно-аппаратные компоненты служб ДТС должны обеспечивать функционирование точки доступа в режиме 24/7/365 с заданной производительностью (в зависимости от планируемого объема проверяемых документов).

4.1.7. Точка доступа должна быть развернута на базе организации, имеющей необходимые лицензии и сертификаты в области защиты информации, выданные соответствующим компетентным органом страны размещения.

4.1.8. Помещения, используемые организацией, обеспечивающей работоспособность точки доступа должны обеспечивать защиту от НСД, гарантированное электропитание и кондиционирование.

4.1.9. Точка доступа ДТС должна вести реестр доказательств, отправляемых и получаемых между участниками трансграничного взаимодействия.

4.2. Требования по реализации Web-служб проверки ЭП

4.2.1. Проверка ЭП должна быть реализована с использованием соответствующих средств криптографической защиты информации и должна состоять из следующих этапов:

4.2.1.1. Проверка корректности формата подписи.

4.2.1.2. Криптографическая проверка ЭП.

4.2.1.3. Проверка действительности сертификата ключа проверки подписи на момент подписи.

4.2.1.4. Проверка наличия корневого сертификата издателя сертификата подписи в списке доверенных сертификатов (TSL).

В случае ошибок при проверке на любом из перечисленных шагов, подпись считается недействительной, а итоговый результат проверки подписи отрицательным.

4.2.1.5. Формирование квитанции о проверке ЭП.

4.2.2. Требования к DVCS серверу.

4.2.2.1. DVCS сервер должен предоставлять сервис в соответствии с протоколом, определенному в RFC 3029 как протокол «подтверждения подлинности электронного документа, подписанного ЭЦП» (Validation of Digitally Signed Document) – vsd-протокол.

4.2.2.2. DVCS сервер должен функционировать в режиме работы, обеспечивающем формирование запросов и выдачу ответов в рамках одной HTTP сессии (синхронный режим).

4.2.2.3. DVCS сервер должен обрабатывать запросы, поступающие посредством протокола HTTP или HTTPS, имеющие Content-Type: application/dvcs.

4.2.2.4. DVCS сервер должен предусматривать возможность авторизации пользователей посредством протокола TLS с использованием соответствующих криптографических стандартов.

4.2.2.5. Должна быть предусмотрена возможность использования разных сертификатов для подписи квитанций и организации TLS-соединения.

4.2.2.6. Все получаемые запросы и формируемые ответы должны быть инкапсулированы в PKCS7 SignedData.

4.2.2.7. DVCS сервер должен проверять все подписи, присоединенные к подписанному документу в части криптографической корректности подписей , а также действительности сертификатов ключей проверки подписи, которыми подписан документ.

4.2.2.8. При проверке действительности сертификатов подписи, DVCS сервер должен полагаться на соответствующие списки отзывов сертификатов (CRLs) или на текущую статусную информацию, полученную от центров сертификации, например от OCSP службы.

4.2.2.9. VSD заявка должна быть сформирована в соответствии с RFC 3029 и содержать:

- уникальный номер VSD-заявки (GUID);
- дату-время генерации VSD-заявки;
- подписанный ЭД в формате, описанном в п. 4.7.1;

- ЭП VSD-заявки, выработанную на ключе подписи пользователя.

4.2.2.10. DVCS сервер в результате проверки ЭД, полученного из VSD-запроса пользователя должен формировать VSD-квитанцию, соответствующую требованиям RFC 3029 и содержащую результат проверки легитимности ЭД, указанного в VSD-заявке (ЭП ЭД действительна или ЭП ЭД недействительна с указанием кода ошибки согласно RFC 3029).

4.2.2.11. VSD-квитанция должна содержать:

- уникальный номер VSD-квитанции (GUID);
- дату и время генерации VSD-квитанции (или штамп времени);
- номер обработанного VSD-запроса;
- подписанный ЭД, полученный в VSD-запросе;
- результат проверки легитимности ЭД (ЭП действительна или ЭП недействительна) на момент выработки ЭП автором ЭД;
- ЭП VSD-квитанции, выработанная на ключе подписи DVCS-сервера.

4.2.2.12. DVCS сервер должен формировать в VSD-квитанциях код возврата (результат проверки ЭП ЭД) в поле status структуры PKIStatusInfo, содержащий результат проверки ЭП ЭД, согласно требованиям RFC 2510 (CMP).

4.2.3. Требования к DSS серверу.

4.2.3.1. DSS сервер должен предоставлять сервис проверки подписи (Verifying Protocol) в соответствии со стандартом Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0 (DSS), определенным в рекомендациях консорциума OASIS.

4.2.3.2. DSS сервер должен функционировать в режиме работы, обеспечивающем формирование запросов и выдачу ответов в рамках одной HTTP сессии (синхронный режим).

4.2.3.3. DSS сервер должен обрабатывать запросы, поступающие посредством протокола HTTP или HTTPS, имеющие Content-Type: application/xml.

4.2.3.4. DSS сервер должен предусматривать возможность авторизации пользователей посредством протокола TLS с использованием российских криптографических стандартов.

4.2.3.5. Должна быть предусмотрена возможность использования разных сертификатов для подписи квитанций и организации TLS-соединения.

4.2.3.6. Все получаемые запросы и формируемые ответы (квитанции) должны представлять из себя подписанные XML-документы.

4.2.3.7. DSS сервер должен проверять все подписи, присоединенные к подписанному документу, используя всю соответствующую информацию о статусах и открытых ключах сертификатов.

4.2.3.8. DSS сервер должен проверять криптографическую корректность всех подписей присоединенных к документу, а также проверять действительность сертификатов подписи, которыми подписан документ.

4.2.3.9. При проверке действительности сертификатов подписи, DSS сервер должен полагаться на соответствующие списки отзывов сертификатов (CRLs) или статусную информацию, полученную от центров сертификации, например от OCSP службы.

4.2.3.10. DSS сервер должен обрабатывать запросы на проверку подписи, в которых поле <ds:Signature> встречается только один раз в запросе.

4.2.3.11. DSS запрос должен представлять из себя подписанный XML документ (со схемой xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema") и содержать следующую информацию:

- уникальный номер запроса (GUID);
- подписанный ЭД;
- ЭД (опционально, в случае подписи отдельно от данных);
- ЭП DSS квитанции, выработанную на ключе подписи DSS сервера (схема xmlns:ds="http://www.w3.org/2000/09/xmldsig#").

4.2.3.12. DSS сервер в результате проверки ЭП, полученной в DSS запросе должен формировать квитанцию, представляющую из себя подписанный XML документ (со схемой xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"), и содержать следующую информацию:

- уникальный номер ответа (GUID);
- статус проверки (ResultMajor, ResultMinor);
- ЭП DSS квитанции, выработанную на ключе подписи DSS сервера (схема xmlns:ds="http://www.w3.org/2000/09/xmldsig#").

4.3. Требования по реализации Web-служб проверки сертификата подписи

4.3.1. Проверка сертификата подписи должна быть реализована с использованием соответствующих средств криптографической защиты информации и должна состоять из следующих этапов:

4.3.1.1. Построение цепочки доверия сертификата.

4.3.1.2. Проверка наличия корневого сертификата издателя сертификата подписи в списке доверенных сертификатов (TSL).

В случае ошибок при проверке на любом из перечисленных шагов, подпись считается недействительной, а итоговый результат проверки подписи отрицательным.

4.3.1.3. Формирование квитанции о проверке ЭП.

4.3.2. Требования к XKMS серверу.

4.3.2.1. XKMS сервер должен предоставлять сервис проверки сертификата (XKISS: Validate Service).

4.3.2.2. XKMS сервер должен функционировать в режиме работы, обеспечивающем формирование запросов и выдачу ответов в рамках одной HTTP сессии (синхронный режим).

4.3.2.3. XKMS сервер должен обрабатывать запросы поступающие посредством протокола HTTP или HTTPS, имеющие Content-Type: application/x-xkms+xml.

4.3.2.4. XKMS сервер должен предусматривать возможность авторизации пользователей посредством протокола TLS с использованием принятых криптографических стандартов.

4.3.2.5. Должна быть предусмотрена возможность использования разных сертификатов для подписи квитанций и организации TLS-соединения.

4.3.2.6. Все получаемые запросы и формируемые ответы (квитанции) должны представлять из себя подписанные XML-документы.

4.3.2.7. При проверке действительности сертификатов подписи, XKMS сервер должен полагаться на соответствующие списки отзывов сертификатов (CRLs) или на текущую статусную информацию, полученную от центров сертификации, например от OCSP службы.

4.3.2.8. XKMS запрос должен представлять из себя подписанный XML документ (со схемой xmlns="http://www.w3.org/2002/03/xkms#") и содержать следующую информацию:

- уникальный номер запроса (GUID);
- сертификат подписи;
- ЭП DSS квитанции, выработанную на ключе подписи DSS сервера (схема xmlns:ds="http://www.w3.org/2000/09/xmldsig#").

4.3.2.9. XKMS сервер в результате проверки ЭП, полученной в DSS запросе, должен формировать квитанцию, представляющую из себя подписанный XML документ (со схемой xmlns="http://www.w3.org/2002/03/xkms#") и содержать следующую информацию:

- уникальный номер ответа (GUID);
- статус ответа (ResultMajor);
- статус проверки сертификата;
- ЭП XKMS квитанции, выработанную на ключе подписи XKMS сервера (схема xmlns:ds="http://www.w3.org/2000/09/xmldsig#").

4.4. Требования по работе со списком статусов доверенных сервисов

4.4.1. Утилита генерации и проверки TSL-списка должна генерировать TSL список, содержащий следующую информацию:

4.4.1.1. Список сертификатов доверенных УЦ с информацией об их классах (квалифицированный, неквалифицированный).

4.4.2. Должен быть разработан программный интерфейс проверки наличия корневого сертификата в TSL.

4.4.3. Проверка TSL списка должна состоять из следующих проверок:

4.4.3.1. Проверка ЭП под TSL списком (схема xmlns:ds="http://www.w3.org/2000/09/xmldsig#").

4.4.3.2. Проверка соответствия TSL списка схеме xmlns:tsl="http://uri.etsi.org/02231/v2#"/.

4.4.4. Должна быть предусмотрена возможность визуализации TSL-списка с отображением следующей информации:

4.4.4.1. Временной интервал, на котором действителен TSL.

4.4.4.2. Название списка

4.4.4.3. Порядковый номер списка

4.4.4.4. Список доверенных корневых сертификатов с указанием общего имени (DN), серийного номера, временного интервала действия сертификата и предоставляемых сервисов.

4.5. Требования по реализации клиентского программного обеспечения для доступа к службам проверки подписи и проверки сертификатов

4.5.1. Требования к DVCS клиенту.

4.5.1.1. Должен обеспечивать формирование VSD-запросов на проверку подписи в соответствии с RFC 3029, содержащим:

- уникальный номер VSD-заявки (GUID);
- дату-время генерации VSD-заявки;
- подписанный ЭД в формате, описанном в п. 4.7.1;

4.5.1.2. Должен обеспечивать подпись VSD запроса с использованием клиентского сертификата.

4.5.1.3. Возможность сохранения VSD запроса.

4.5.1.4. Должен отправлять VSD запрос на заданный сервер по протоколу HTTPS с Content-Type: application/dvcs.

4.5.1.5. Должен предоставлять функции получения и загрузки VSD ответа.

4.5.1.6. Должен предоставлять функции проверки VSD ответа.

4.5.1.7. Должен предоставлять функцию получения статуса проверки ЭП в VSD ответе.

4.5.1.8. Возможность сохранения VSD ответа в файл.

4.5.1.9. Возможность визуального просмотра VSD ответа.

4.5.2. Требования к DSS клиенту.

4.5.2.1. Должен обеспечивать формирование DSS-запросов на проверку подписи в соответствии с в соответствии со спецификациями OASIS DSS (OASIS Digital Signature Service) и соответствующих схеме данных xmlns:dss="urn:oasis:names:tc:dss:1.0:core:schema"), содержащим следующую информацию:

- уникальный номер запроса (GUID);
- подписанный ЭД;
- ЭД (опционально, в случае подписи отдельно от данных);
- ЭП DSS квитанции, выработанную на ключе подписи DSS сервера (схема xmlns:ds="http://www.w3.org/2000/09/xmldsig#").

4.5.2.2. Должен обеспечивать подпись DSS запроса с использованием клиентского сертификата.

4.5.2.3. Возможность сохранения DSS запроса в файл.

4.5.2.4. Должен отправлять DSS запрос на заданный сервер по протоколу HTTPS с Content-Type: application/xml.

4.5.2.5. Должен предоставлять функции получения и загрузки DSS ответа.

4.5.2.6. Должен предоставлять функции проверки DSS ответа.

4.5.2.7. Должен предоставлять функцию получения статуса проверки ЭП в DSS ответе.

4.5.2.8. Возможность сохранения DSS ответа в файл.

4.5.2.9. Возможность визуального просмотра DSS ответа.

4.5.3. Требования к XKMS клиенту

4.6. Должен обеспечивать формирование XKMS-запросов на проверку подписи в соответствии со спецификациями XKMS v2.0 (XML Key Management Specification) и соответствующих схеме данных xmlns="http://www.w3.org/2002/03/xkms#"), содержащим следующую информацию:

- уникальный номер запроса (GUID);
- один или несколько сертификатов подписи;
- ЭП DSS квитанции, выработанную на ключе подписи DSS сервера (схема xmlns:ds="http://www.w3.org/2000/09/xmldsig#").

4.6.1.1. Должен обеспечивать подпись XKMS запроса с использованием клиентского сертификата.

4.6.1.2. Возможность сохранения XKMS запроса в файл.

4.6.1.3. Должен отправлять XKMS запрос на заданный сервер по протоколу HTTPS с Content-Type: application/x-xkms+xml.

4.6.1.4. Должен предоставлять функции получения и загрузки XKMS ответа.

4.6.1.5. Должен предоставлять функции проверки XKMS ответа.

4.6.1.6. Должен предоставлять функцию получения статуса проверки сертификата в XKMS ответе.

4.6.1.7. Возможность сохранения XKMS ответа в файл.

4.6.1.8. Возможность визуального просмотра XKMS ответа.

4.7. Требования к информационному обеспечению

4.7.1. Рекомендуется к использованию единый формат ЭП, содержащий в себе доказательства времени подписи (в соответствии с RFC 3161 «Internet X.509 Public Key Infrastructure Time-Stamp Protocol – TSP») и доказательства действительности сертификата подписи на момент подписи (в соответствии с RFC 2560 «Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP»). Формат электронных сообщений должен соответствовать формату «подписанных данных» (SignedData) стандарта PKCS#7 в соответствии с требованиями RFC 2630 (CMS).

4.7.1.1. ЭП электронных документов вырабатывается от хэш-значения общей части электронного документа (содержания), вычисленного как deattached signature (отсоединенная ЭП).

4.7.1.2. Реализация хэш функции и ЭП должна соответствовать форматам, принятым в соответствующей системе электронного документооборота.

4.7.1.3. Электронное сообщение должно содержать сертификат подписи.

4.7.1.4. Штамп времени помещается в неподписываемый атрибут сообщения с OID равным «1.2.840.113549.1.9.16.2.14».

4.7.1.5. OCSP-ответ помещается в закодированном виде (BIT string) в неподписываемый атрибут сообщения с OID равным «1.2.840.113549.1.9.16.2.22».

4.7.2. Службы проверки ЭП и сертификатов подписи должны вести реестры запросов проверки документов, а также реестр выдаваемых квитанций о фактах и результатах проверки.

5. Рекомендации по функциональности программного модуля, предназначенного для встраивания в системы электронного документооборота участников трансграничного электронного взаимодействия и организующего взаимодействие с соответствующими службами ДТС

5.1. В программном модуле реализуются следующие функции:

5.1.1. Доставка из системы электронного документооборота электронного документа (ЭД), подписанного иностранной электронной подписью;
5.1.2. Определение типа подписи ЭД;
5.1.3. Формирование запроса к ДТС для подтверждения легитимности подписи;
5.1.4. Получение ответа на запрос от ДТС («квитанции») либо исходного документа, подписанного электронной подписью ДТС.

5.2. Программный модуль должен предоставлять следующие возможности программного шлюза для организации единых точек входа к службе ДТС для обработки ЭД с иностранной ЭП:

5.2.1. Основные процедуры проверки электронных подписей (см. п.4.2.1).
5.2.2. Получение квитанции от ДТС о проверке электронной подписи.
5.2.3. Запрос на проверку подписи иностранного государства и переподписывание документа электронной подписью ДТС.
5.2.4. Отправка в ДТС документа для его подписи с использованием выбранного крипто провайдера.
5.2.5. Возможность гибкой настройки при добавлении новых средств электронной подписи.
5.2.6. Возможность работы в асинхронном или синхронном режимах.
5.2.7. Загрузка актуального списка доверенных сертификатов (TSL - Trust-service Status List) и списков отозванных сертификатов (COC) для реализации проверки электронных подписей.
5.2.8. Предоставление защищенного доступа к службам ДТС в соответствии с ролями (пользователь, администратор) с использованием сертификатов ключей подписи по протоколу TLS (Transport Layer Security).
5.2.9. Протоколирование операций проверки ЭП.
5.2.10. Сбор информации о производительности.

5.3. Состав программного модуля:

5.3.1. Серверная компонента, встраиваемая в состав СЭДО и отвечающая за распознавание поступающих в СЭДО электронных документов, подписанных иностранной ЭП.

Серверная компонента выполняет следующие функции:

- Формирование ЭП документов в формате, принятом в СЭДО.
- Определение документов, подписанных иностранными электронными подписями и формирование в зависимости от типа подписи и политик использования по необходимому протоколу (OASIS DSS, XKMS, RFC 3029) взаимодействия соответствующего запроса к ДТС для подтверждения легитимности подписи.

- Взаимодействие с низкоуровневыми компонентами используемого крипто провайдера (например, КриптоПро CSP) и API служб валидации ЭЦП.
- Проверка и разбор квитанций о проверке документов, полученных от ДТС.
- Передачу в АРМ доступа квитанций служб валидации для сохранения и дальнейшего возможного использования при разборе конфликтных ситуаций.

5.3.2. Клиентская компонента, предоставляющая пользователю СЭДО адресованные ему электронные документы, подписанные иностранной ЭП, с отметкой (квитанцией) службы ДТС об их легитимности. Электронный документ с иностранной ЭП признается легитимным для использования в СЭДО стороны-получателя, если результат проверки данной ЭП является положительным. Клиентская компонента должна реализовывать функцию доставки ЭД и сообщения о его легитимности пользователю СЭДО - получателю ЭД. Сообщение подписывается соответствующим сертификатом.

Основные функции клиентской компоненты:

- Функция проверки сертификата подписи в соответствии со списками доверенных Удостоверяющих Центров (Trusted Service List – далее TSL), формат которых должен соответствовать спецификации ETSI TS 102 231 «Electronic Signatures and Infrastructures (ESI). Provision of harmonized Trust-service status information»;
- Функция проверки ЭП документа на основании представленного документа и подписи под ним.
- Функция проверки ЭП документа на основании предоставленного хэша документа и подписи под документом.
- Функция проверки штампа времени.

5.3.2.1. Клиентская компонента предоставляет программные интерфейсы взаимодействия со службой валидации сертификатов, базирующиеся на спецификации XKMS v2.0 (XML Key Management Specification) и обеспечивающие:

- Генерацию заявок на проверку сертификата ключа подписи.
- Отправку по защищенному каналу в соответствии с настроенными политиками XKMS-запросов на службу валидации сертификатов ДТС.
- Получение XKMS-квитанций, содержащих результаты проверки сертификата;
- Разбор XKMS-квитанций и проверка ЭЦП под квитанциями службы валидации сертификатов ДТС.

5.3.2.2. Клиентская компонента реализовывает программный интерфейс взаимодействия со службой валидации ЭП ДТС, базирующийся на спецификации OASIS DSS (OASIS Digital Signature Service), обеспечивающий:

- Генерацию заявок на проверку ЭП документа на основании документа и подписи под ними.

- Генерацию заявок на проверку ЭП документа на основании хэша документа и подписи под ним.
- Отправку по защищенному каналу в соответствии с настроенными политиками DSS-запросов на службу валидации ДТС.
- Получение DSS-квитанций, содержащих результаты проверки всех ЭП, присоединенных к отправленному DSS-запросу;
- Разбор DSS-квитанций и проверка ЭП под квитанциями службы валидации ЭП ДТС.

5.3.2.3. Программный модуль предоставляет программные интерфейсы взаимодействия со службой валидации ЭП, базирующиеся на спецификации X842 – RFC 3029 «Internet X.509 Public Key Infrastructure. Data Validation and Certification Server Protocols» со следующими функциональными возможностями:

- Генерация заявок на проверку ЭП документа на основании документа и подписи под ними.
- Генерация заявок на проверку ЭП документа на основании хэша документа и подписи под ним.
- Отправка по защищенному каналу в соответствии с настроенными политиками VSD-запросов на службу валидации ЭП.
- Получение VSD -квитанций, содержащих результаты проверки всех ЭП, присоединенных к отправленному VSD -запросу;
- Разбор VSD -квитанций и проверка ЭП под квитанциями службы валидации ЭП.

5.4. Пример использования программного модуля, предназначенного для встраивания в системы ЭДО.

В качестве примера использования программного модуля можно рассмотреть построение информационного и технологического взаимодействия СЭДО, применяемой при организации грузовых перевозок в ОАО «РЖД» (АС «ЭТРАН») с программно-аппаратным комплексом ДТС, функционирующим на базе УЦ ОАО «НИИАС». Главной целью построения взаимодействия являлась возможность обработки в АС ЭТРАН (без дополнительных действий со стороны пользователя) ЭД, подписанных иностранной ЭЦП.

Был разработан макет программно-аппаратного комплекса, обеспечивающего признание электронных подписей (далее – Макет) при трансграничном электронном документообороте (использовались крипто провайдер и другие программные продукты ООО «КРИПТОПРО»). Макет содержит АРМ с возможностью подключения к АС ЭТРАН (АРМ доступа), на котором устанавливается клиентская компонента для взаимодействия АРМ доступа с сервисами ДТС, функционирующими на базе УЦ ОАО «НИИАС». Проведена адаптация АРМ доступа в составе АС «ЭТРАН», организовано взаимодействия АРМ доступа с сервисами ДТС.

В качестве аппаратной платформы для функционирования встраиваемого программного модуля использован сервер HP Proliant DL380R07 с процессором Intel Pentium с частотой 2.4 ГГц и с 4 Гб оперативной памяти.

В качестве программной платформы использована операционная система Microsoft Windows Server 2003 (x86) с установленным пакетом обновлений SP2 и выше или Microsoft Windows Server 2008 (x86 или x64) с установленным пакетом обновлений SP2 и выше или Microsoft Windows Server 2008 R2 с установленным пакетом обновлений SP1 и выше.

На компьютере (сервере), предназначенном для функционирования программного модуля, установлено следующее ПО:

- крипто провайдер (для проверки документов, подписанных ЭП с использованием необходимых крипто алгоритмов, а также для возможности формирования ответных квитанций);
- программное обеспечение, реализующее протокол TSP на клиентском рабочем месте (TSP Client).
- программное обеспечение, реализующее протокол OCSP на клиентском рабочем месте (OCSP Client).
- Microsoft SQL Server 2008 R2 (может быть установлена на другом сервере).

Тестирование работоспособности Макета проводилось на полигоне ГО «Белорусская железная дорога» (БЧ) - ОАО «РЖД», где была реализована предложенная белорусской стороной концепция технического решения парной ДТС, построенной в соответствии с международными рекомендациями и спецификациями ITU-T X.842 (см. п. 6.3.1).

Функциональная схема Макета представлена на рисунке 1.

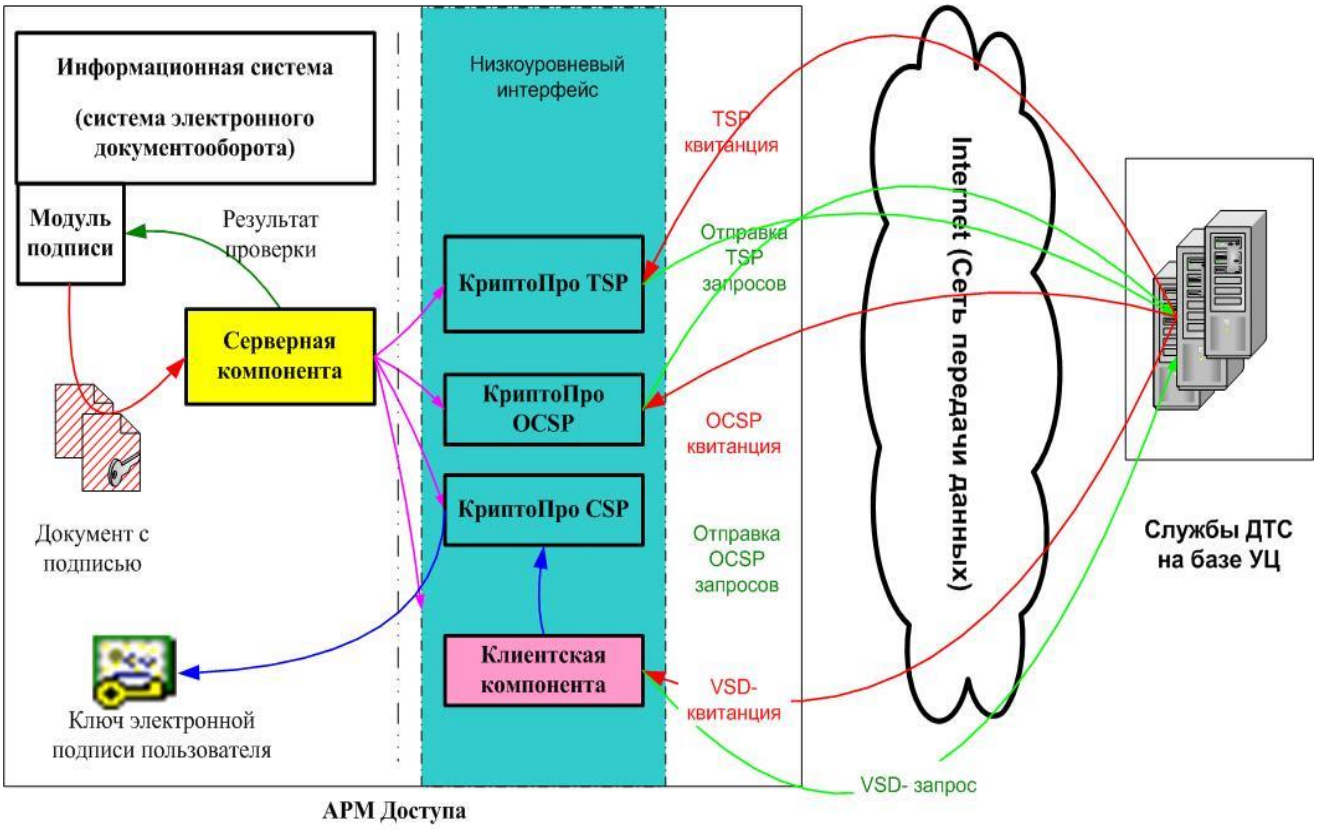


Рис 3. Функциональная схема

5.5. Рекомендации по организации трансграничного взаимодействия с зарубежными партнерами посредством EDI-системы.

Типовая схема взаимодействия через EDI-систему с использованием сервисов ДТС представлена на рисунке 4 и предполагает возможность прозрачного использования сервисов ДТС, не затрагивая основного функционала EDI-систем участников взаимодействия.

Для работы необходимо выделение следующих очередей в EDI-системе для каждого участника:

1. Очередь для черновиков документов. В данную очередь помещаются не подписанные документы в формате IFTMIN, подготовленные в АС стороны отправителя, а также подписанные документы от отправителя.
2. Очередь для обработанных документов. В данную очередь помещаются документы IFTMIN отправителя со снятой ЭП (в случае положительного результата проверки).

5.5.1. Рекомендации по подписи документов при экспорте

Подпись и отправку документов для экспорта рекомендуется формировать на основании ранее сформированных подписей грузоотправителей, товарных кассиров и других ответственных лиц. Рекомендуется назначить ответственное лицо в организации для подписи трансграничных документов, которое в автоматизированном режиме (серверная подпись с соблюдением необходимых мер информационной безопасности по доступу и хранению ключевой информации) будет обеспечивать подпись документов.

Рекомендуемый алгоритм работы модуля взаимодействия с ДТС. Выполняются следующие шаги (обозначены на схеме кружками с цифрами на белом фоне):

1. Программный модуль взаимодействия с ДТС просматривает очередь входящих IFTMIN документов, загружает и регистрирует их в соответствии с уникальным идентификатором документа IFTMIN (из входящей очереди загружаются только IFTMIN документы).
2. Программный модуль взаимодействия с ДТС направляет входящие IFTMIN документы в программный модуль автоматического подписания для подписи документов на закрытом ключе ответственного лица, отвечающего за подпись трансграничных документов Отправителя.

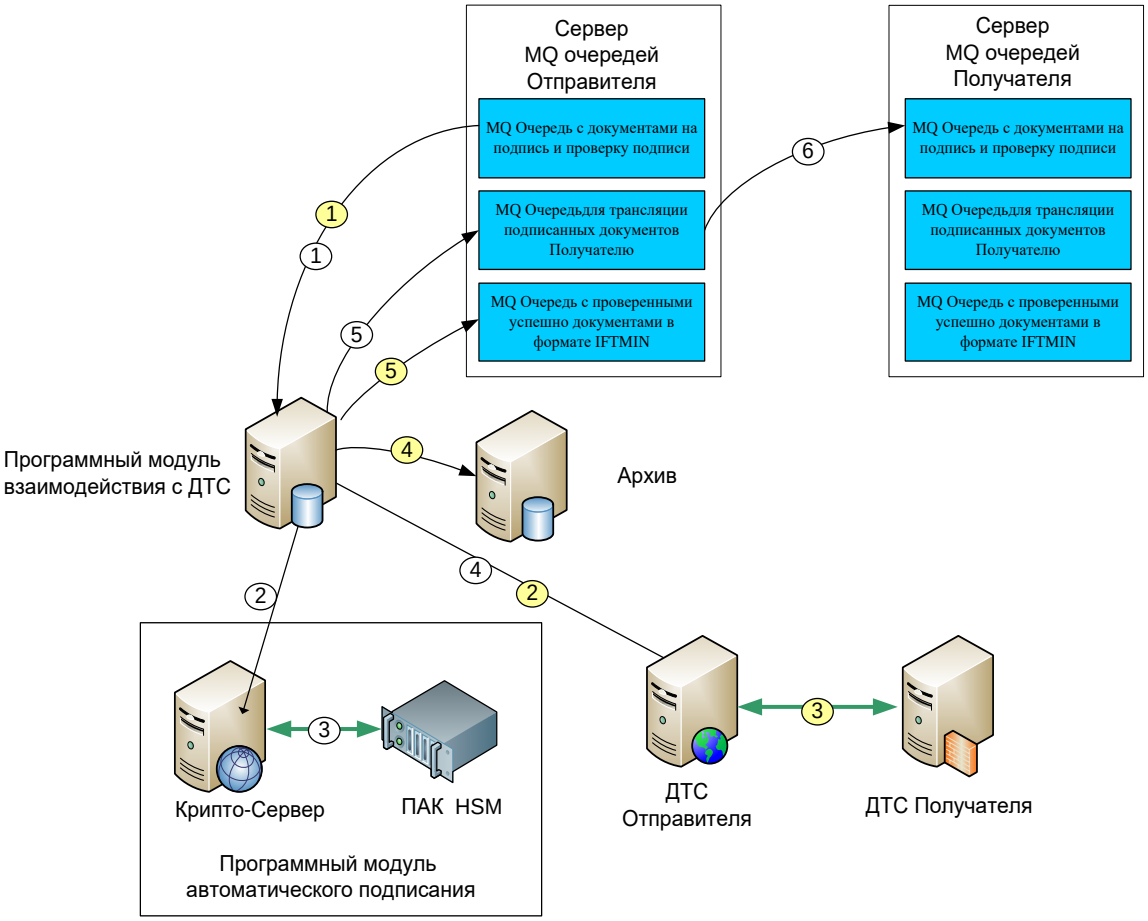


Рис. 4. Использование программного модуля взаимодействия с ДТС в рамках информационного обмена РЖД – Партнер.

3. Модуль автоматического подписания осуществляет подпись документов на закрытом ключе ответственного лица Отправителя. Подпись формируется в формате PKCS#7 совместно с данными.
   Рекомендуется добавление штампов времени и актуальных статусов сертификатов при формировании ЭП.
4. Сформированный таким образом блок с подписью возвращается в программный модуль взаимодействия с ДТС и при необходимости (в зависимости от схемы работы ДТС) отправляется в ДТС своей стороны для получения дополнительных доказательств подписи (в качестве примера можно взять схему взаимодействия РЖД-КТЖ - п.6.3.3).
5. Программный модуль взаимодействия с ДТС передает сформированный блок данных в исходящую MQ очередь, соответствующую получателю IFTMIN-документа.
6. Документ из исходящей очереди передается во входящую очередь получателя.

5.5.2. Рекомендации по проверке подписи при импорте.

Рекомендуемый алгоритм работы модуля взаимодействия с ДТС. Выполняются следующие шаги (обозначены на схеме кружками с цифрами на желтом фоне):

1. Программный модуль взаимодействия с ДТС просматривает очередь входящих подписанных документов, загружает и регистрирует их в соответствии с уникальным идентификатором документа IFTMIN.
2. Программный модуль взаимодействия с ДТС формирует в зависимости от типа подписи соответствующий запрос к ДТС ОАО «РЖД», подписанный на ключе ОАО «РЖД», для подтверждения легитимности подписи под входящим документом.
3. ДТС ОАО «РЖД» при необходимости (в случае отсутствия необходимых доказательств на своей стороне, например, см. схему взаимодействия ДТС-БЧ, п.6.3.1) на основании полученного запроса формирует запрос и направляет его в ДТС Партнера. ДТС Партнера обрабатывает полученный запрос, и направляет обратно в ДТС ОАО «РЖД» соответствующий ответ, подписанный на своем ключе RSA.

   ДТС ОАО «РЖД» на основании полученного ответа от ДТС Партнера и соответствующей квитанции формирует квитанцию о проверке, подписанную своим ключом (с помощью программного модуля автоматического подписания).
4. Программный модуль взаимодействия с ДТС помещает в архив полученную квитанцию и проверяемый входящий документ IFTMIN.
5. В случае получения положительного ответа по факту проверки подписи, программный модуль взаимодействия с ДТС передает документ IFTMIN в формате EDIFACT в исходящую очередь с успешно проверенными документами.

6. Архитектура и модели доверия «инфраструктур открытых ключей» участников трансграничного электронного взаимодействия

6.1. Сервисы службы ДТС.

Служба ДТС предоставляет сервисы, указанные в Таблице 1.

Таблица 1 – Сервисы Службы ДТС.

Подсистема Службы	**Порт**	**Краткая характеристика сервиса**
Публичный веб-сервер	80	Гипертекстовый интерфейс к публично доступной информации о представленном сервисе.
Веб-интерфейс доступа к функционалу сервиса ДТС	443 (TLS с аутентификацией клиента) и/или 80	Гипертекстовый интерфейс по приему заявок и возврату квитанций пользователям сервиса.

Приведенный список сервисов и портов служит информацией для конфигурирования внешних средств защиты, например, брандмауэров или пакетных фильтров.

6.2. Служба ДТС построена по модульному принципу и содержит в своем составе следующие подсистемы:

6.2.1. Модуль разграничения доступа для протокола HTTP.

6.2.2. Веб-серверы для предоставления информации, или выступающие в роли графического веб-интерфейса к службам сервиса или отвечающие за транспортировку информации:

6.2.2.1. Публичный веб-сервер Службы ДТС.

6.2.2.2. Веб-сервер, поддерживающий транспортировку запросов на сервис и квитанций пользователю.

6.2.2.3. Веб-сервер, реализующий графический интерфейс к персональным страницам пользователей Службы.

6.2.3. Репозиторий сервиса.

6.2.4. Средства криптографической защиты информации.

6.2.5. Модуль функциональной поддержки.

6.2.6. Фискальная подсистема.

6.2.7. Абонентский пункт администраторов сервиса.

6.2.8. Консольное рабочее место администратора сервиса.

6.2.9. Утилита командной строки – программное обеспечение пользователей сервиса TTP.

Транспортировка информации к/от Службы ДТС для протоколов DVCS и OCSP, а также для задач административного управления, осуществляется по протоколу HTTP, инкапсулированному в TLS. Субъектами доступа (ресурсами) выступают веб-сервера. Разграничение доступа к ресурсам основано на свойствах защищенного

протокола TLS, поддерживаемых специальным модулем разграничения доступа для протокола HTTP.

Исходя из вышеизложенного, интерфейс по осуществлению защищенного доступа и взаимодействия пользователей со Службой ДТС включает:

- средства криптографической защиты информации;
- протоколы HTTP, HTTPS;
- протокол TLS, обеспечивающий защищённую передачу данных;
- протокол OCSP;
- протокол TSP;
- протокол DVCS;
- веб-серверы;
- средства отображения информации – браузеры;
- форматы и коды – HTML;
- отображаемую информацию – веб-сайты и веб-страницы;
- веб-приложения и утилиту командной строки, реализующие диалоги, взаимодействие и транзакции между пользователем и веб-серверами, обратную связь с пользователем;
- абонентский пункт администраторов сервиса и консольное рабочее место администратора сервиса, реализующие средства для администрирования Службы ДТС;
- порядок использования Службы ДТС и документацию на нее.

6.3. Модели доверия «Инфраструктур открытых ключей» участников трансграничного электронного взаимодействия.

На сегодняшний день получен практический опыт реализации трансграничной электронной подписи с использованием сервисов ДТС, в частности, в технологии безбумажной перевозки вагонов и грузов по электронным юридически значимым документам в международном сообщении между ОАО «РЖД» и БЧ, ОАО «РЖД» и Государственной администрацией железнодорожного транспорта Украины («Укрзализныця»), ОАО «РЖД» и АО «НК «КТЖ»,.

Дополнительно подписаны соглашения по схеме парных ДТС между ОАО «РЖД» и АО ЭВР, ЛДЗ, АО «УБЖД».

В настоящее время реализовано три модели организации проверки электронных документов:

- Схема парных ДТС.
- Схема взаимодействия доверенных УЦ.
- Модифицированная схема парных ДТС с пред квитированием.

Далее более подробно рассматриваются модели доверия в перечисленных случаях трансграничного электронного взаимодействия.

6.3.1. Трансграничный юридически значимый электронный документооборот по схеме парных ДТС

В настоящее время схема парных ДТС реализована между ОАО «РЖД», БЧ, ЛГ и КТЖ.

Трансграничный электронный документооборот между ОАО «РЖД» и БЧ осуществляется в рамках Соглашения об осуществлении перевозок приватных вагонов по безбумажной технологии с использованием электронного документооборота между Российской Федерацией и Республикой Беларусь (приложение № 5 к Соглашению между открытым акционерным обществом «Российские железные дороги» и Государственным объединением Белорусская железная дорога об электронном обмене данными при перевозках грузов в международном железнодорожном сообщении от 28 июля 2004 г. № 520).

Трансграничный электронный документооборот между ОАО «РЖД» и ЛГ осуществляется в рамках Соглашения об осуществлении перевозок приватных вагонов по безбумажной технологии с использованием электронного документооборота из Литовской Республики в Российскую Федерацию (Соглашение между открытым акционерным обществом «Российские железные дороги» и АО «Литовские железные дороги» от 04 октября 2012 г. № 949). Трансграничный электронный документооборот между ОАО «РЖД» и КТЖ осуществляется в рамках Соглашения об осуществлении перевозок приватных вагонов по безбумажной технологии с использованием электронной накладной между Акционерным обществом «КТЖ – Грузовые перевозки» и Открытым акционерным обществом «Российские железные дороги» (Соглашение между открытым акционерным обществом «Российские железные дороги» и Акционерным обществом «КТЖ – Грузовые перевозки» от 16 ноября 2016 г. № 11/62-ГП/135).

Предложенное техническое решение предполагает, что каждый из пользователей информационного обмена работает исключительно с ДТС своего домена с учетом локальных требований национального законодательства и требований соглашения о взаимодействии с ДТС. Сама же ЭП (ЭЦП) проверяется в том домене, в котором выпущен сертификат автора, а сопредельной стороной не проверяется. Доверие к электронному документу у принимающей стороны основывается на квитанции ее ДТС, сформированной по результатам проверки ЭП (ЭЦП) под документом, осуществленной ДТС стороны-отправителя. Для организации между ДТС доверенного канала связи используется протокол TLS с использованием аутентификация сторон по сертификатам, выпущенным на базе криптографического алгоритма RSA.

При этом информационный обмен между комплексами ДТС (запросы и ответы) осуществляется с использованием электронной подписи, сформированной на базе криптографического алгоритма RSA с применением алгоритма хеширования SHA-1, а между соответствующими ДТС и информационными системами железных дорог - с использованием национальных криптографических алгоритмов, легитимных в соответствующем правовом поле.

В качестве примера применения технологии на рис. 5 представлен механизм взаимодействия информационных систем железных дорог в направлении Россия – Белоруссия , который включает следующие основные этапы:

1. В АС ЭТРАН на станции отправления подготавливается электронная накладная с ЭП, предназначенная для трансграничной передачи.
2. После оформления электронной накладной с ЭП в АС ЭТРАН на станции отправления данные об отправке, включая признак электронности, передаются в EDI-систему.

3. На пограничной станции после проведения необходимых процедур в соответствии с технологическим процессом работы станции по факту «раскредитования» электронной накладной из АС ЭТРАН передаются в EDI-систему сведения из этой накладной с признаком электронности и статусом «раскредитована».
4. По факту получения электронной накладной со статусом «раскредитована» и признаком электронности EDI-система формирует сообщение IFTMIN, которое направляется для автоматического подписания электронной подписью на сертификате уполномоченного лица ОАО «РЖД».

Общая схема трансграничного взаимодействия информационных систем при обмене электронными сообщениями, содержащими ЭП/ЭЦП, между ОАО «РЖД» и БЧ

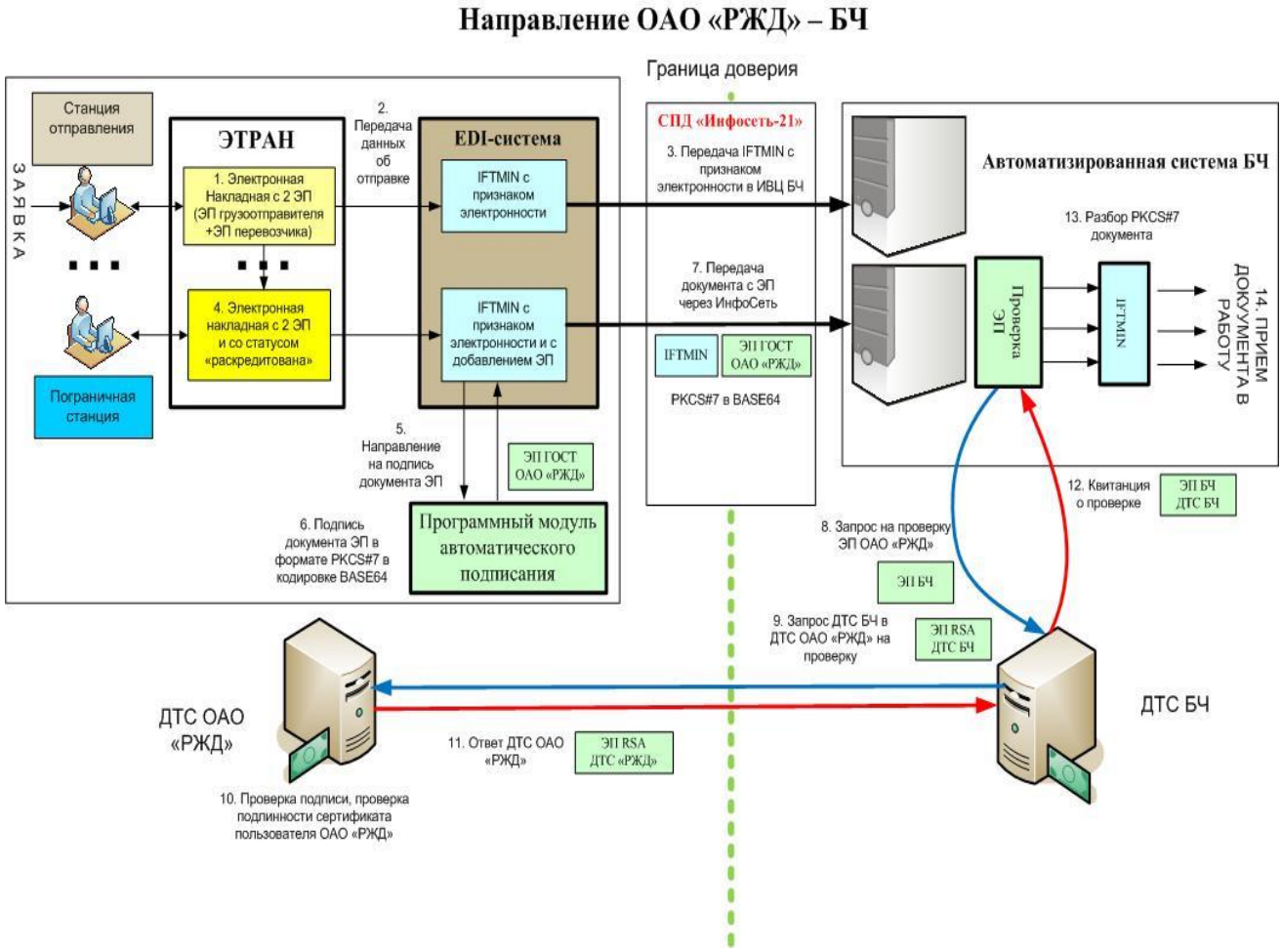


Рис.5. Общая схема трансграничного взаимодействия информационных систем при обмене электронными документами, содержащими ЭП, между ОАО «РЖД» и БЧ (направление Россия-Белоруссия).

5. Текстовый документ в формате IFTMIN подписывается на ключе, предназначенном для подписи трансграничных документов. Подпись формируется в формате PKCS#7 совместно с данными. Подпись должна содержать доказательство времени подписи (штамп времени).
6. Посредством EDIFACT документ передается через транспортную подсистему EDI-системы в СПД «Инфосеть-21» и далее в автоматизированную систему (АС) БЧ.

7. АС БЧ формирует запрос на проверку подписи ОАО «РЖД», подписывает его ключом пользователя БЧ и передает его на проверку в ДТС БЧ.
8. ДТС БЧ на основании запроса пользователя БЧ формирует запрос на проверку подписи ОАО «РЖД», подписывает его на ключе RSA и отправляет его в ДТС ОАО «РЖД».
9. ДТС ОАО «РЖД» проверяет переданную ему подпись и подлинность сертификата пользователя ОАО «РЖД».
10. ДТС ОАО «РЖД» отправляет квитанцию о проведенной проверке в ДТС БЧ, подписанную ключом RSA.
11. На основании полученной от ДТС ОАО «РЖД» квитанции ДТС БЧ формирует квитанцию для пользователя БЧ, подписанную сертификатом ДТС БЧ на национальном алгоритме республики Беларусь.
12. АС БЧ извлекает из PKCS#7 документа содержимое в формате IFTMIN и передает его адресату на дальнейшую обработку.
13. Адресат – пользователь АС БЧ принимает документ в работу в соответствии с принятыми бизнес процессами.

Механизм взаимодействия информационных систем железных дорог в направлении Белоруссия - Россия представлен на рис.6 и включает следующие основные этапы:

1. АС БЧ формирует заявку для трансграничного взаимодействия.
2. Сформированная заявка преобразуется в сообщение IFTMIN (формат UN/EDIFACT).
3. Текстовый документ в формате UN/EDIFACT подписывается на ключе ответственного лица БЧ, назначенного ответственным за подпись трансграничных документов. Подпись формируется в формате PKCS#7 совместно с данными. Подпись должна содержать доказательство времени подписи (штамп времени).
4. Посредством EDI-системы документ передается через Инфосеть в АС ОАО «РЖД».
5. Далее документ попадает в программный модуль взаимодействия с ДТС, описанный в разделе 6 настоящего документа, который формирует запрос на проверку подписи БЧ, подписывает его ключом пользователя ОАО «РЖД» и передает его на проверку в ДТС ОАО «РЖД».

Общая схема трансграничного взаимодействия информационных систем при обмене электронными сообщениями, содержащими ЭП/ЭЦП, между ОАО «РЖД» и БЧ

Направление БЧ – ОАО «РЖД»

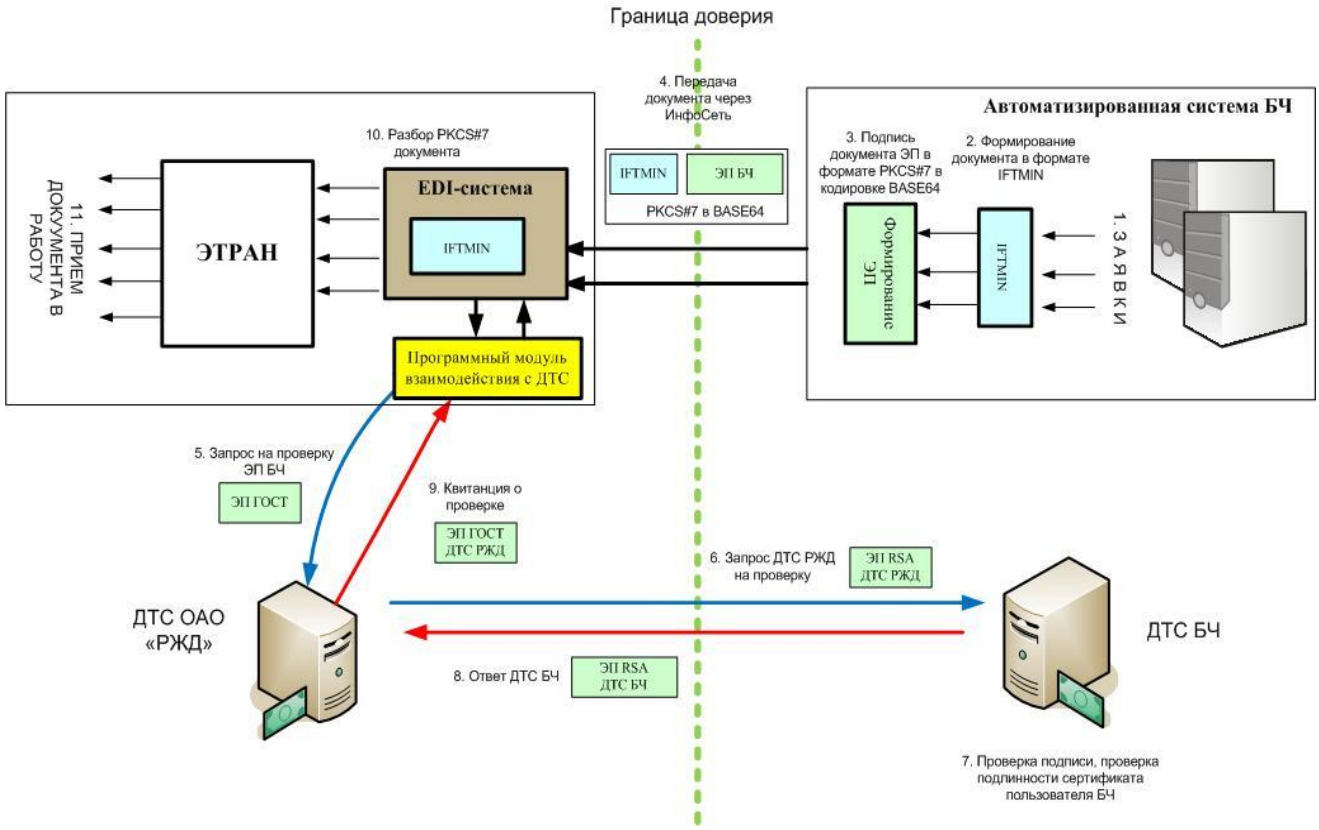


Рис.6. Общая схема трансграничного взаимодействия информационных систем при обмене электронными документами, содержащими ЭП, между ОАО «РЖД» и БЧ (направление Белоруссия-Россия).

6. ДТС ОАО «РЖД» на основании запроса пользователя ОАО «РЖД» формирует запрос на проверку подписи БЧ, подписывает его на ключе RSA и отправляет его в в ДТС БЧ.
7. ДТС БЧ проверяет переданную ему подпись, подлинность сертификата пользователя БЧ.
8. ДТС БЧ отправляет квитанцию о проведенной проверке в ДТС ОАО «РЖД», подписанную ключом RSA.
9. На основании полученной от ДТС БЧ квитанции ДТС ОАО «РЖД» формирует квитанцию для пользователя ОАО «РЖД», подписанную сертификатом ДТС ОАО «РЖД» с использованием российских криптографических алгоритмов.
10. Программный модуль взаимодействия с ДТС извлекает из PKCS#7 документа содержимое сообщения IFTMIN и передает его на дальнейшую обработку.
11. Адресат – пользователь АС ЭТРАН принимает документ в работу в соответствии с принятыми бизнес процессами.

6.3.2. Трансграничный юридически значимый электронный документооборот по схеме взаимодействия доверенных УЦ

В настоящее время схема взаимодействия доверенных УЦ реализована между ОАО «РЖД» и УЗ.

В соответствии с подписанным «Соглашением об осуществлении перевозок приватных порожних вагонов по безбумажной технологии с использованием электронного документооборота между Украиной и Российской Федерацией» от 21.01.2013 осуществляются перевозки порожних приватных вагонов между ОАО «РЖД» и УЗ с использованием электронной накладной.

При взаимодействии с УЗ (аналогично взаимодействию с БЧ) накладные СМГС передаются в виде электронных документов в формате UN/EDIFACT (сообщение IFTMIN) по каналам сети «Инфосеть-21».

В отличие от варианта парных ДТС, при взаимодействии с УЗ проверка электронной подписи не требует использования технологии ДТС и базируется на взаимодействии доверенных удостоверяющих центров (ДУЦ) сторон, обмене национальными криптографическими алгоритмами и средствами электронной подписи.

ЭП, используемая во внутренних информационных системах сторон (грузоперевозчиков, товарных агентов), не передается сопредельной стороне. Для трансграничной передачи стороной-отправителем формируется сообщение IFTMIN, содержащее признак электронности и подписываемое на ее ключе ЭП, предназначенном для трансграничного взаимодействия, а также на ключе ЭП, предоставленном взаимодействующей стороной. Данное сообщение IFTMIN передается через EDI-систему совместно со сформированными на нем ЭП.

Доверие к полученному документу основывается на проверке двух ЭП под сообщением IFTMIN, доставленным стороне-получателю. Проверка включает в себя также запрос на проверку действительности сертификата в ДУЦ стороны-отправителя.

Успешный результат проверки обеих ЭП позволяет ДУЦ получающей стороны сформировать квитанцию для адресата документа, свидетельствующую о возможности приема документа в дальнейшую работу.

Более подробно механизм взаимодействия выглядит в направлении Россия – Украина следующим образом (рис.7).

Предварительным этапом, предшествующим началу обмена электронными перевозочными документами, является обмен средствами ЭП, ключами и сертификатами доверенных удостоверяющих центров сторон (шаг 0).

Общая схема трансграничного взаимодействия информационных систем при обмене электронными сообщениями, содержащими ЭП, между ОАО «РЖД» и УЗ

Направление Россия – Украина

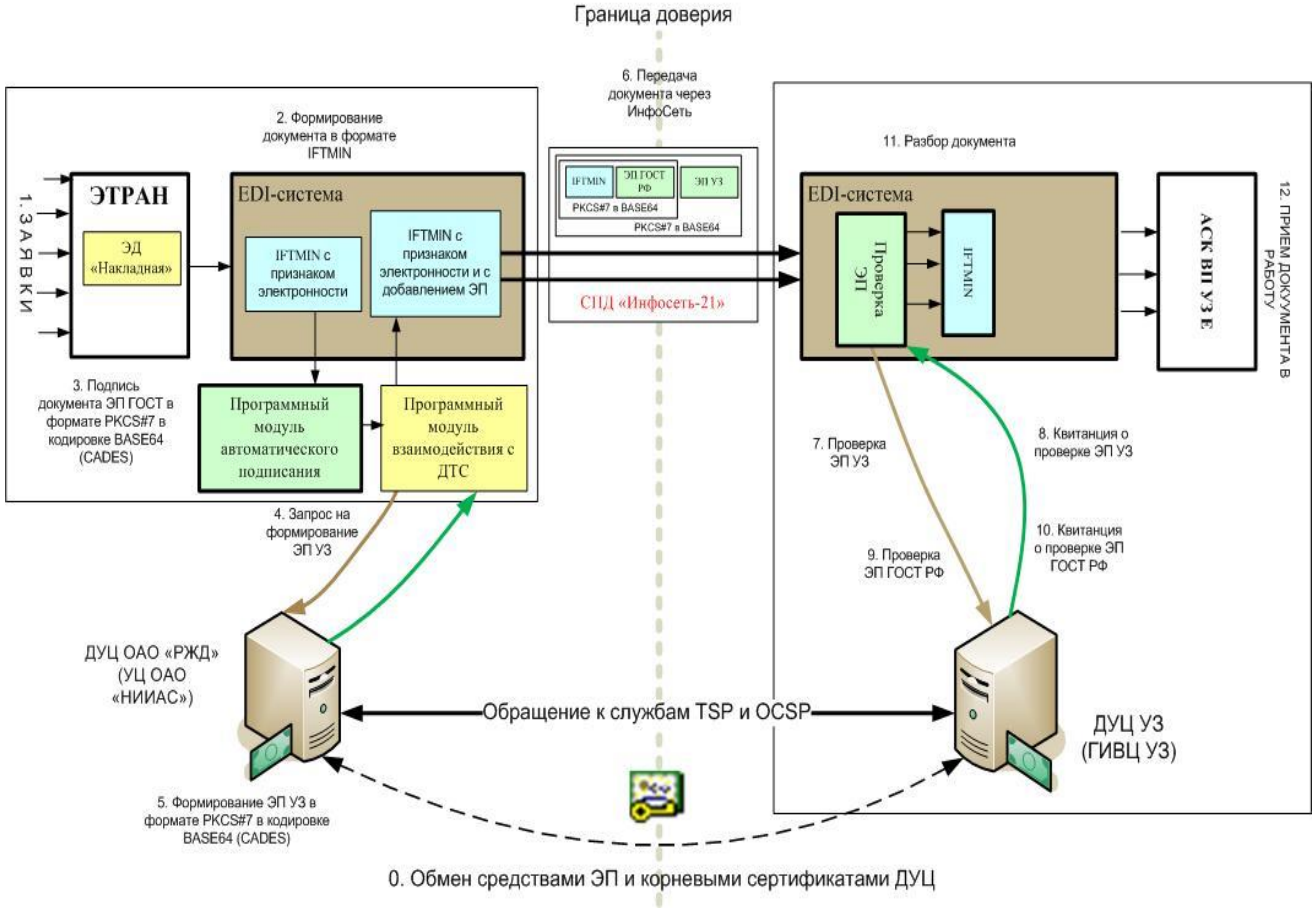


Рис.7. Общая схема трансграничного взаимодействия информационных систем при обмене электронными документами, содержащими ЭП, между ОАО «РЖД» и УЗ (направление Россия-Украина).

1. В АС ЭТРАН на основе поступающих заявок подготавливается электронная накладная, предназначенная для трансграничной передачи.
2. В EDI-системе формируется сообщение IFTMIN (железнодорожная накладная) с признаком электронности.
3. EDI-система направляет данное сообщение IFTMIN для автоматического подписания электронной подписью на ключе ОАО «РЖД», предназначенном для подписи трансграничных документов. Подпись формируется в формате PKCS#7 совместно с данными и штампом времени (формат CADES).
4. Программный модуль взаимодействия с ДТС направляет запрос в ДУЦ ОАО «РЖД» на формирование ЭП на ключе, предоставленном УЗ.
5. ДУЦ ОАО «РЖД» формирует ЭП на ключе, предоставленном УЗ, в формате PKCS#7 в кодировке BASE64(CADES) и возвращает подписанный документ в EDI-систему.

6. Посредством EDIFACT документ передается через транспортную подсистему EDI-системы в СПД «Инфосеть-21» и далее в автоматизированную систему (АС) УЗ.
7. АС УЗ формирует запрос на проверку подписи УЗ под полученным сообщением и передает его на проверку в ДУЦ УЗ.
8. ДУЦ УЗ осуществляет проверку ЭП УЗ и направляет квитанцию о ее результатах в АС УЗ.
9. Аналогичным образом АС УЗ направляет запрос на проверку подписи ОАО «РЖД».
10. На основании проведенной проверки ЭП ОАО «РЖД» ДУЦ УЗ формирует квитанцию для пользователя УЗ, подписанную сертификатом ДУЦ УЗ.
11. АС УЗ извлекает из PKCS#7 документа содержимое в формате IFTMIN и передает его адресату на дальнейшую обработку.
12. Адресат – пользователь АС УЗ принимает документ в работу в соответствии с принятыми бизнес процессами.

На рисунке 8 представлен механизм взаимодействия в направлении Украина – Россия. Предварительным этапом, предшествующим началу обмена электронными перевозочными документами, является обмен средствами ЭП, ключами и сертификатами доверенных удостоверяющих центров сторон (шаг 0).

Общая схема трансграничного взаимодействия информационных систем при обмене электронными сообщениями, содержащими ЭП, между ОАО «РЖД» и УЗ

Направление Украина - Россия

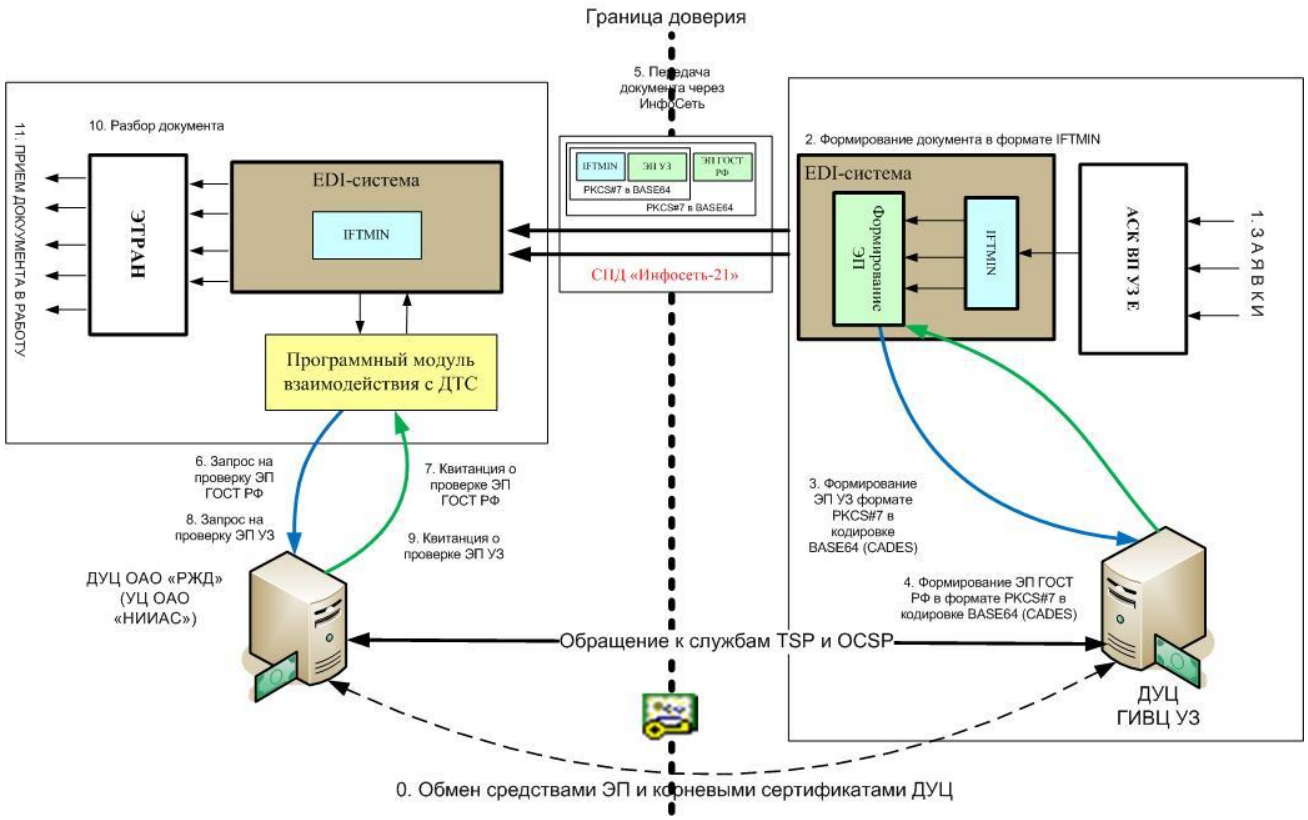


Рис.8. Общая схема трансграничного взаимодействия информационных систем при обмене электронными документами, содержащими ЭП, между ОАО «РЖД» и УЗ (направление Украина - Россия).

1. В АС УЗ подготавливается электронная накладная, предназначенная для трансграничной передачи.
2. В EDI-системе формируется сообщение IFTMIN (железнодорожная накладная) с признаком электронности.
3. EDI-система направляет данное сообщение IFTMIN в ДУЦ ГИВЦ УЗ для автоматического подписания электронной подписью на ключе УЗ, предназначенном для подписи трансграничных документов. Подпись формируется в формате PKCS#7 совместно с данными и штампом времени (формат CADES).
4. Аналогично направляется запрос на формирование ЭП на российском крипто алгоритме (ГОСТ).
5. Подписанный документ передается через транспортную подсистему EDI-системы в СПД «Инфосеть-21» и далее в EDI-систему ОАО «РЖД».
6. EDI-система ОАО «РЖД» формирует запрос на проверку подписи ГОСТ под полученным сообщением в ДУЦ ОАО «РЖД».
7. ДУЦ ОАО «РЖД» осуществляет проверку ЭП ГОСТ и направляет квитанцию о ее результатах в EDI-систему ОАО «РЖД».
8. Аналогичным образом EDI-система ОАО «РЖД» направляет запрос на проверку подписи УЗ.
9. На основании проведенной проверки ЭП УЗ ДУЦ ОАО «РЖД» формирует квитанцию для пользователя ОАО «РЖД», подписанную своим сертификатом.
10. EDI-система ОАО «РЖД» извлекает из PKCS#7 документа содержимое в формате IFTMIN и передает его в АС ЭТРАН адресату на дальнейшую обработку.
11. Адресат – пользователь АС ЭТРАН принимает документ в работу в соответствии с принятыми бизнес процессами.

6.3.3. Трансграничный юридически значимый электронный документооборот по модифицированной схеме парных ДТС с предквитированием

Модифицированная схема взаимодействия ДТС была разработана совместно с представителями ОАО «РЖД» и КТЖ и предполагает отсутствие связи между ДТС при проверке ЭП.

Предложенное техническое решение предполагает, что каждый из пользователей информационного обмена работает исключительно с ДТС своего домена с учетом локальных требований национального законодательства и требований соглашения о взаимодействии с ДТС. Сама же ЭП (ЭЦП) проверяется в том домене, в котором выпущен сертификат автора, а сопредельной стороной не проверяется. Доверие к электронному документу у принимающей стороны основывается на квитанции ее ДТС, сформированной по результатам проверки ЭП (ЭЦП) под документом, осуществленной ДТС стороны-отправителя.

При этом информационный обмен между комплексами ДТС (запросы и ответы) осуществляется с использованием электронной подписи, сформированной на базе криптографического алгоритма RSA с применением алгоритма хеширования SHA-1, а между соответствующими ДТС и информационными системами железных дорог - с использованием национальных криптографических алгоритмов, легитимных в соответствующем правовом поле.

Отличительной особенностью Данной схемы является отсутствие прямой связи между ДТС Сторон. ДТС-квитанции передающей стороны формируются не в момент проверки подписи на принимающей стороне, а в момент подписи на передающей. Соответствующее доказательство прикрепляется к передаваемому документу и направляется принимающей стороне.

Более подробно механизм взаимодействия представлен на примере направления Россия – Казахстан[1] следующим образом (рис.8).

Общая схема трансграничного взаимодействия информационных систем при обмене электронными сообщениями, содержащими ЭП/ЭЦП, между ОАО «РЖД» и АО «НК «КТЖ»

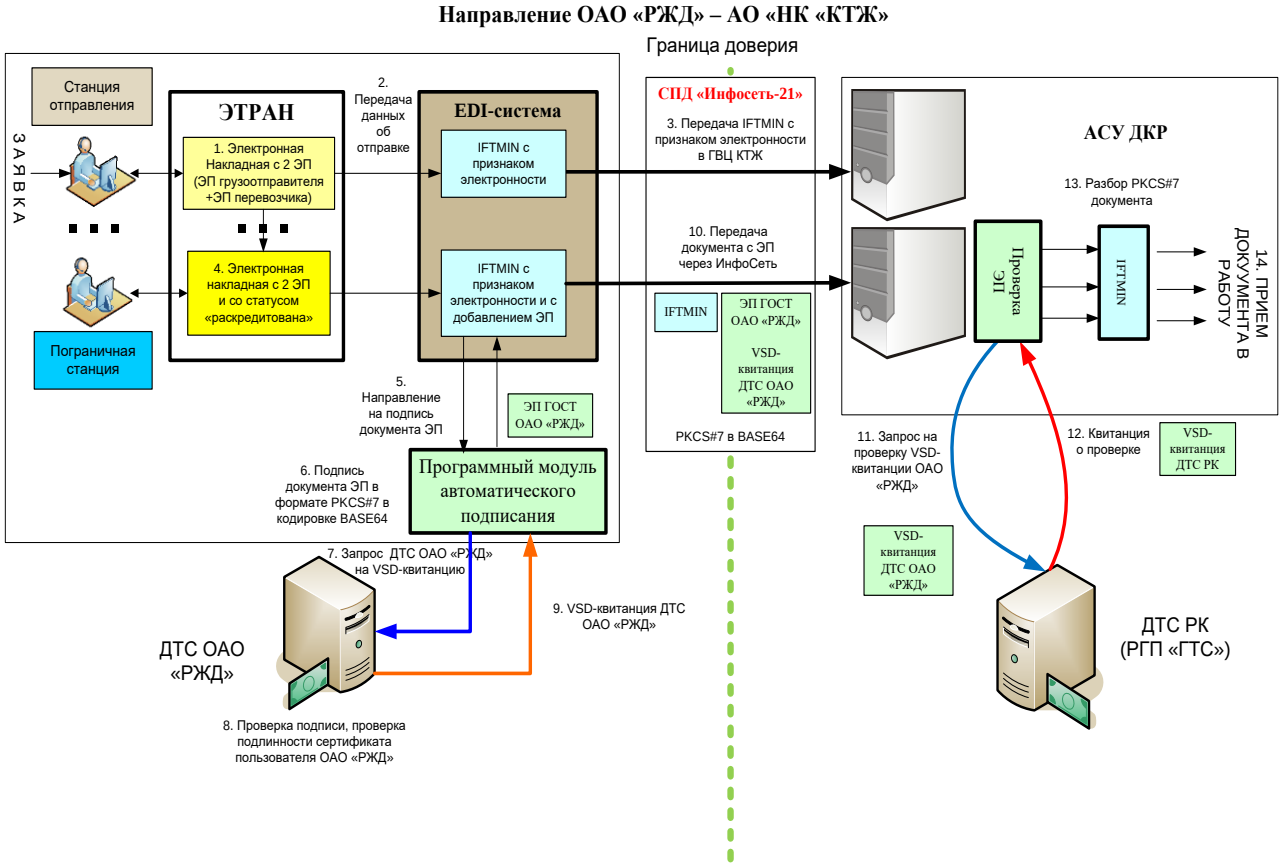


Рис.8. Общая схема трансграничного взаимодействия информационных систем при обмене электронными документами, содержащими ЭП, между ОАО «РЖД» и КТЖ (направление Россия-Казахстан).

[1] В настоящее время между КТЖ и ОАО «РЖД» используется схема парных ДТС.

1. В АС ЭТРАН на основе поступающих заявок подготавливается электронная накладная, предназначенная для трансграничной передачи.
2. После оформления электронной накладной с ЭП в АС ЭТРАН на станции отправления данные об отправке, включая признак электронности, передаются в EDI-систему.
3. В EDI-системе формируется сообщение IFTMIN (железнодорожная накладная) с признаком электронности, которое передается по действующей технологии и в соответствии с подписанным соглашением об ЭОД в ГВЦ КТЖ по факту оформления перевозочного документа на станции приема груза к перевозке (информация об отправке).
4. На пограничной станции после проведения необходимых процедур в соответствии с технологическим процессом работы станции по факту «раскредитования» электронной накладной из АС ЭТРАН передаются в EDI-систему сведения из этой накладной с признаком электронности и статусом «раскредитована».
5. По факту получения электронной накладной со статусом «раскредитована» и признаком электронности EDI-система формирует сообщение IFTMIN, которое направляется для автоматического подписания электронной подписью на сертификате уполномоченного лица ОАО «РЖД».
6. Текстовый документ в формате IFTMIN подписывается на ключе, предназначенном для подписи трансграничных документов. Подпись формируется в формате PKCS#7 совместно с данными. Подпись должна содержать доказательство времени подписи (штамп времени).
7. Программный модуль автоматического подписания направляет запрос в ДТС ОАО «РЖД» на формирование квитанции проверки ЭП ОАО «РЖД».
8. ДТС ОАО «РЖД» проверяет подпись под ЭД и формирует VSD-квитанцию о проверке, подписанную на RSA ключе.
9. VSD-квитанция о проверке ЭП, подписанная на RSA-ключе ДТС ОАО «РЖД», присоединяется к ЭД в неподписываемый атрибут ЭП.
10. Посредством EDIFACT итоговый документ передается через транспортную подсистему EDI-системы в СПД «Инфосеть-21» и далее в автоматизированную систему КТЖ (АСУ ДКР).
11. АС КТЖ извлекает из полученного ЭД VSD-квитанцию о проверке ЭП ОАО «РЖД», подписанную RSA-ключом ДТС ОАО «РЖД», и формирует запрос на ее проверку в ДТС КТЖ.
12. ДТС КТЖ осуществляет проверку квитанции о проверке ЭП, выданной ДТС ОАО «РЖД», и направляет квитанцию о результатах проверки в АСУ ДКР.
13. АСУ ДКР извлекает из PKCS#7 документа содержимое в формате IFTMIN и передает его адресату на дальнейшую обработку.
14. Адресат – пользователь АСУ ДКР принимает документ в работу в соответствии с принятыми бизнес процессами.

Общая схема трансграничного взаимодействия информационных систем при обмене электронными сообщениями, содержащими ЭП/ЭЦП, между ОАО «РЖД» и АО «КТЖ» направление РК-РФ

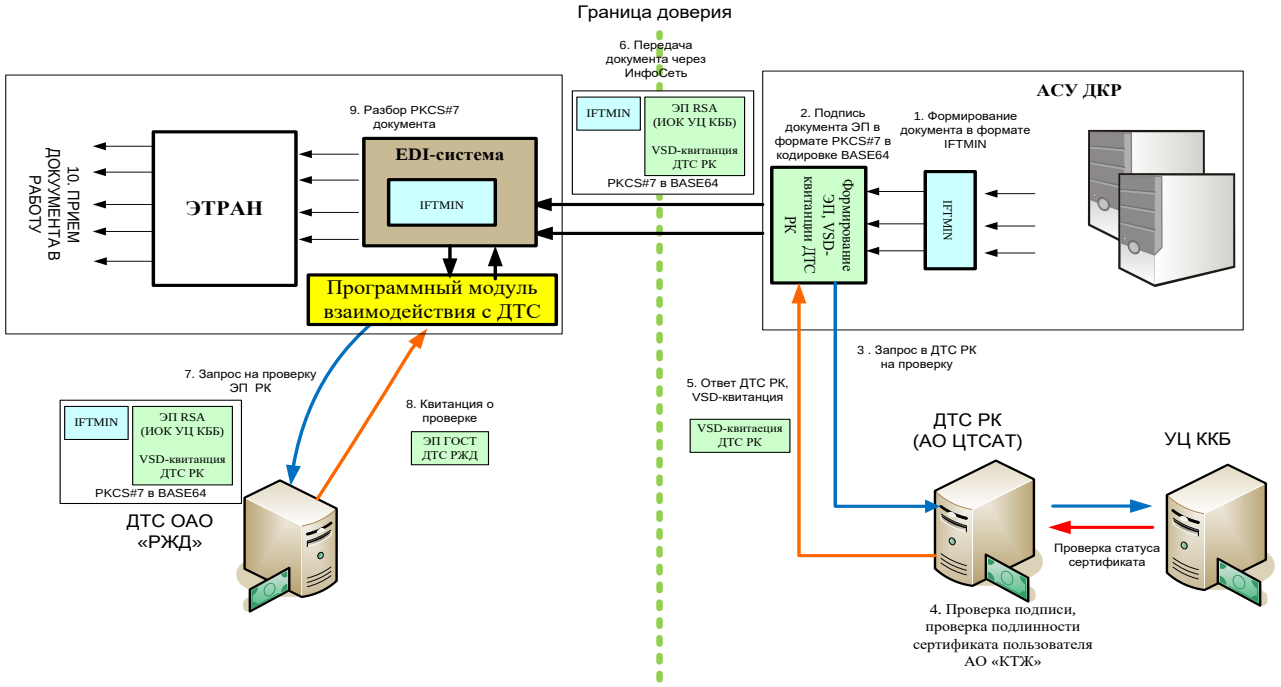


Рис.9. Общая схема трансграничного взаимодействия информационных систем при обмене электронными документами, содержащими ЭП, между ОАО «РЖД» и КТЖ (направление Казахстан - Россия).

На рисунке 9 механизм взаимодействия в направлении Казахстан – Россия.

1. В EDI-системе формируется сообщение IFTMIN (железнодорожная накладная) с признаком электронности.
2. В АСУ ДКР осуществляется подписание IFTMIN сообщения на ключе ответственного сотрудника АС КТЖ.
3. АСУ ДКР формирует и направляет в ДТС КТЖ подписанное сообщение IFTMIN для проверки подписи.
4. ДТС КТЖ проверяет подпись под ЭД и формирует квитанцию о проверке, подписанную на RSA ключе.
5. VSD-квитанция о проверке ЭП, подписанная на RSA-ключе ДТС КТЖ, присоединяется к ЭД в неподписываемый атрибут ЭП.
6. Подписанный документ с квитанцией о проверке передается через транспортную подсистему EDI-системы в СПД «Инфосеть-21» и далее в EDI-систему ОАО «РЖД».
7. EDI-система ОАО «РЖД» формирует запрос на проверку подписи под полученным сообщением в ДТС ОАО «РЖД».
8. ДТС ОАО «РЖД» извлекает из полученного ЭД квитанцию о проверке ЭП КТЖ, подписанную RSA-ключом ДТС КТЖ, осуществляет проверку ее ЭП и направляет квитанцию о результатах проверки ЭП в EDI-систему ОАО «РЖД».
9. EDI-система ОАО «РЖД» извлекает из PKCS#7 документа содержимое в формате IFTMIN и передает его в АС ЭТРАН адресату на дальнейшую обработку.

10. Адресат – пользователь АС ЭТРАН принимает документ в работу в соответствии с принятыми бизнес процессами.

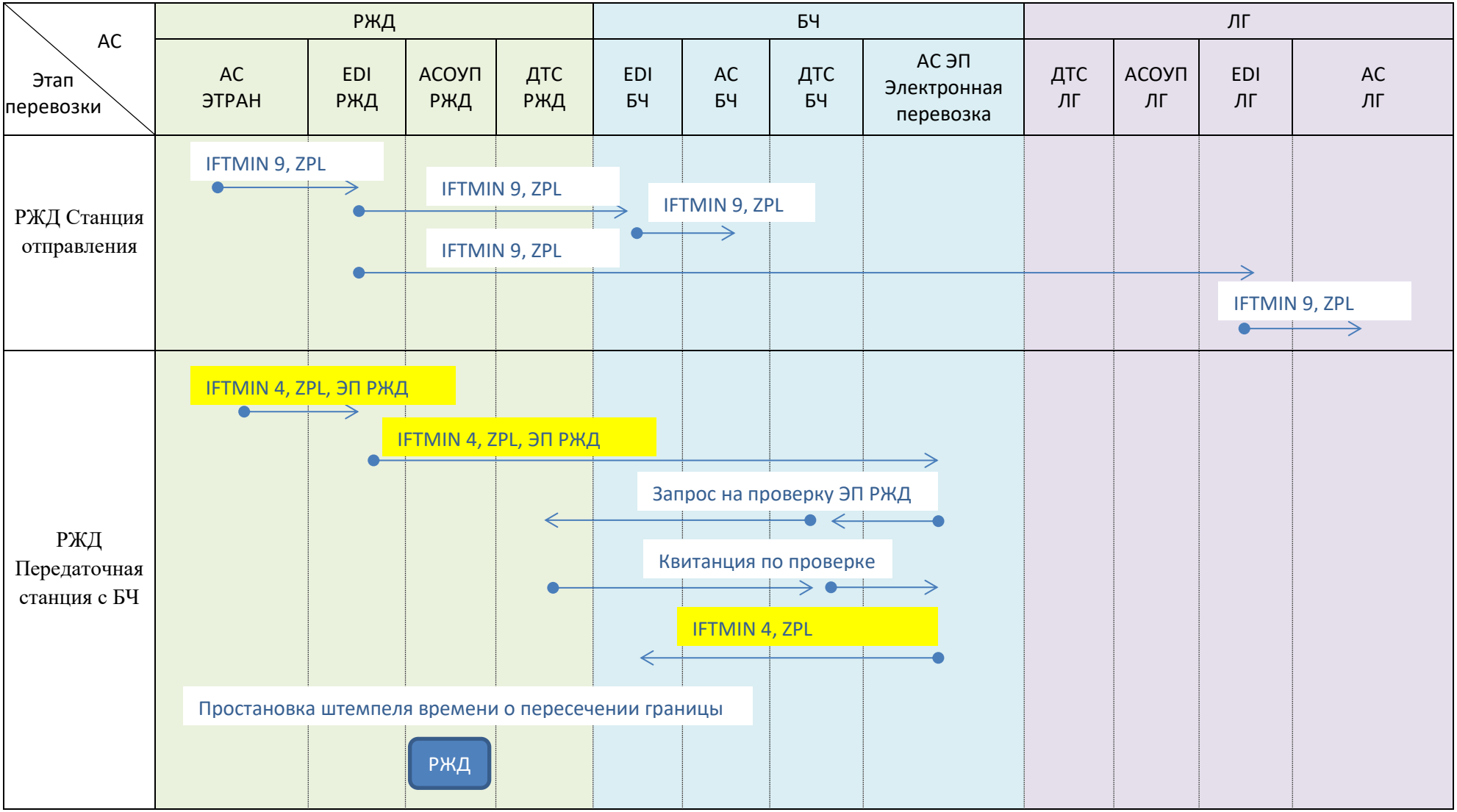
6.4. Взаимное признание ЭП в ЭД, оформленных в правовых полях различных государств, при организации железнодорожных перевозок по цепочкам маршрутов

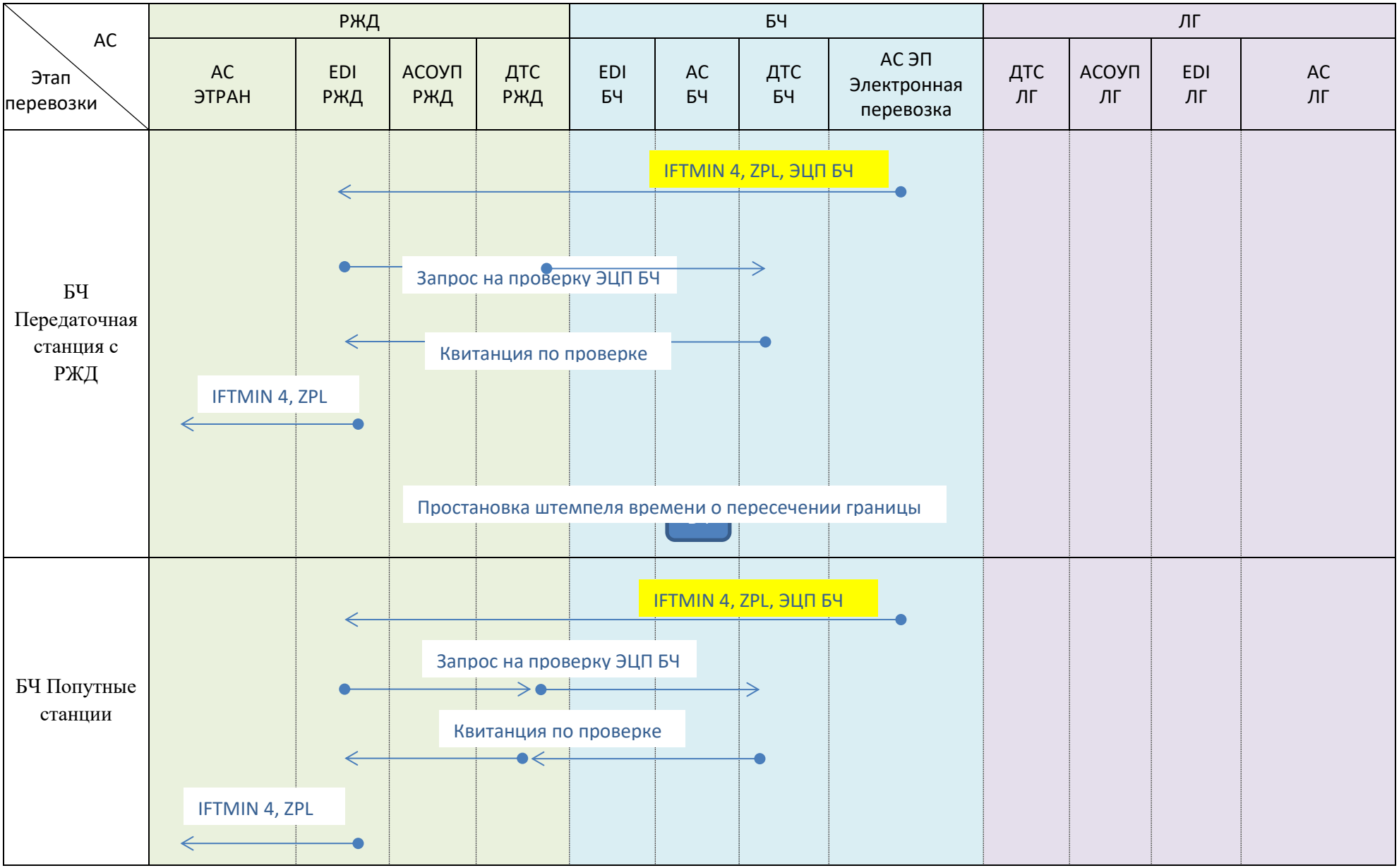
Схема парных ДТС может быть применена, в том числе, и для организации железнодорожных перевозок, включающих транзит через территорию нескольких государств. При этом юридически значимое взаимодействие и подписание ЭД происходит на стыке сопредельных администраций, что в свою очередь позволяет использовать данную схему при наличии только парных связей между сопредельными администрациями, а не всех участников перевозочного процесса.

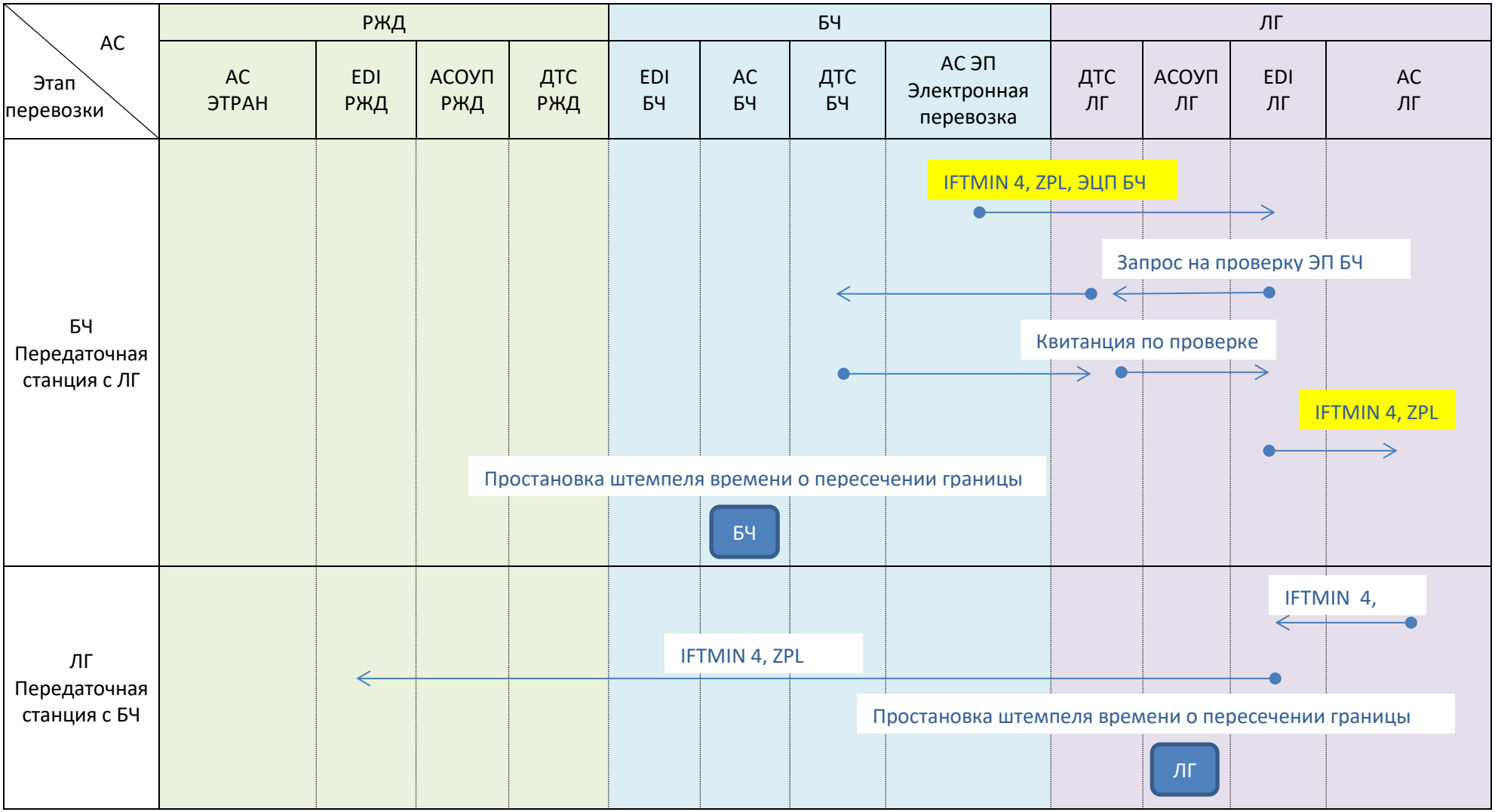
При отсутствии возможности организации связи между ДТС на одном из участков транзита возможно использование бумажного документооборота или схем без участия ДТС.

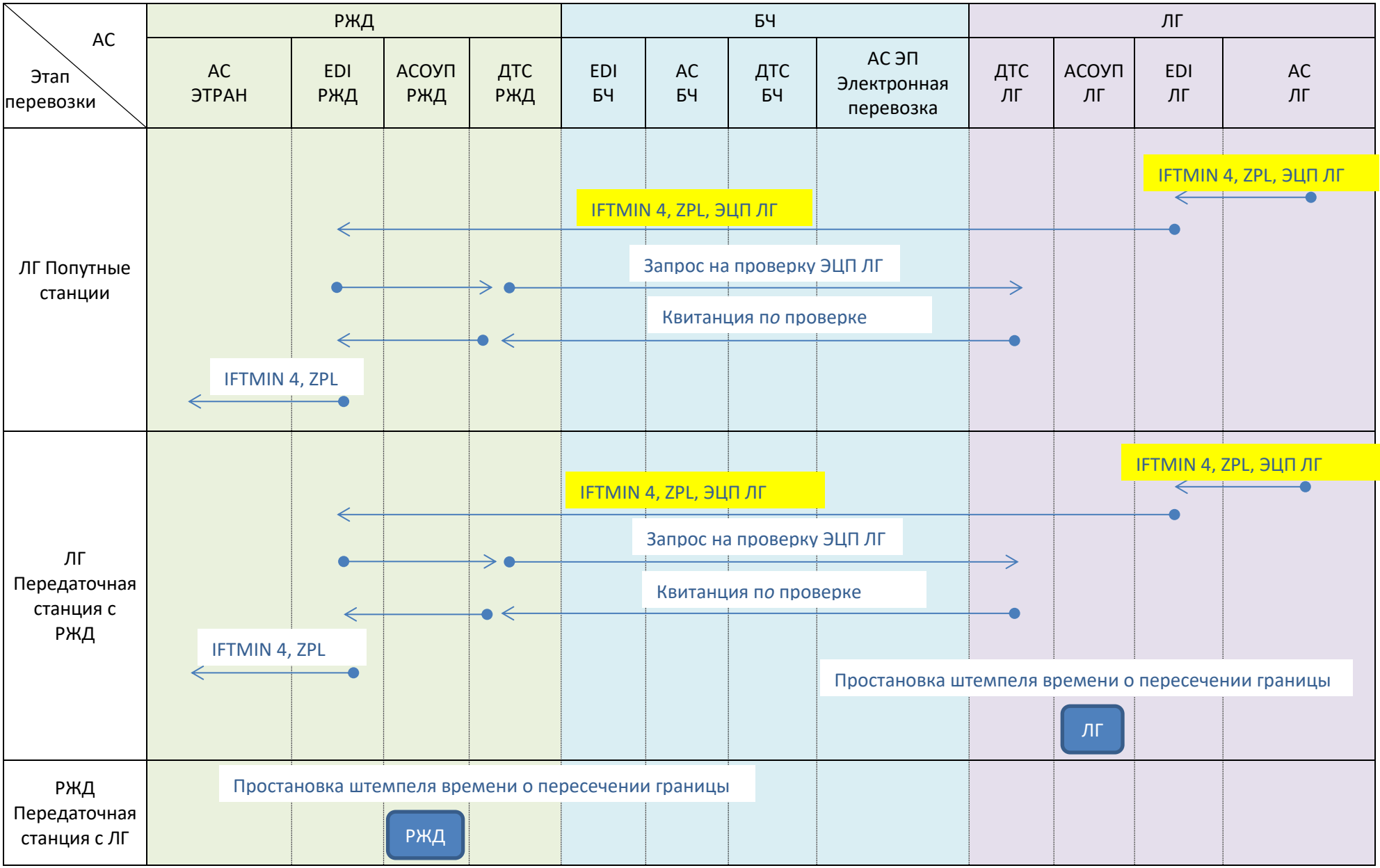
В схеме на Таблице №2 детально описан пример обмена электронными юридически значимыми перевозочными документами при осуществлении транзитных перевозок порожних вагонов по маршруту Россия (КЖД) – Литва – Белоруссия – Россия и в обратном направлении. Юридическая значимость электронных документов, созданных в различных правовых полях, обеспечивается посредством применения технологии парных Доверенных третьих сторон.

Таблица 2. Схема обмена документами при организации цепочек маршрутов




АС
Этап перевозки
РЖД
БЧ
ЛГ
АС ЭТРАН
EDI РЖД
АСОУП РЖД
ДТС РЖД
EDI БЧ
АС БЧ
ДТС БЧ
АС ЭП Электронная перевозка
ДТС ЛГ
АСОУП ЛГ
EDI ЛГ
АС ЛГ
БЧ Передаточная станция с РЖД
IFTMIN 4, ZPL, ЭЦП БЧ
Запрос на проверку ЭЦП БЧ
Квитанция по проверке
IFTMIN 4, ZPL
Простановка штемпеля времени о пересечении границы
БЧ Попутные станции
IFTMIN 4, ZPL, ЭЦП БЧ
Запрос на проверку ЭЦП БЧ
Квитанция по проверке
IFTMIN 4, ZPL


АС
Этап перевозки
РЖД
БЧ
ЛГ
АС ЭТРАН
EDI РЖД
АСОУП РЖД
ДТС РЖД
EDI БЧ
АС БЧ
ДТС БЧ
АС ЭП Электронная перевозка
ДТС ЛГ
АСОУП ЛГ
EDI ЛГ
АС ЛГ
БЧ Передаточная станция с ЛГ
IFTMIN 4, ZPL, ЭЦП БЧ
Запрос на проверку ЭП БЧ
Квитанция по проверке
IFTMIN 4, ZPL
Простановка штемпеля времени о пересечении границы
БЧ
ЛГ Передаточная станция с БЧ
IFTMIN 4,
IFTMIN 4, ZPL
Простановка штемпеля времени о пересечении границы
ЛГ


АС
Этап перевозки
РЖД
БЧ
ЛГ
АС ЭТРАН
EDI РЖД
АСОУП РЖД
ДТС РЖД
EDI БЧ
АС БЧ
ДТС БЧ
АС ЭП Электронная перевозка
ДТС ЛГ
АСОУП ЛГ
EDI ЛГ
АС ЛГ
ЛГ Попутные станции
IFTMIN 4, ZPL, ЭЦП ЛГ
IFTMIN 4, ZPL, ЭЦП ЛГ
Запрос на проверку ЭЦП ЛГ
Квитанция по проверке
IFTMIN 4, ZPL
ЛГ Передаточная станция с РЖД
IFTMIN 4, ZPL, ЭЦП ЛГ
IFTMIN 4, ZPL, ЭЦП ЛГ
Запрос на проверку ЭЦП ЛГ
Квитанция по проверке
IFTMIN 4, ZPL
Простановка штемпеля времени о пересечении границы
ЛГ
РЖД Передаточная станция с ЛГ
Простановка штемпеля времени о пересечении границы
РЖД

АС / Этап перевозки	РЖД				БЧ				ЛГ			
	АС ЭТРАН	EDI РЖД	АСОУП РЖД	ДТС РЖД	EDI БЧ	АС БЧ	ДТС БЧ	АС ЭП Электронная перевозка	ДТС ЛГ	АСОУП ЛГ	EDI ЛГ	АС ЛГ
РЖД станция назначения (КЖД)	Штемпели времени о пересечении границ ←											

7. Требования к узлам инфраструктуры доверия – комплексам ДТС

7.1. Юридические аспекты трансграничного взаимодействия в соответствии с требованиями законодательств страны - резидента ДТС.

Внедрение электронного документооборота в сегменте международных ж/д перевозок сдерживается по ряду причин, основной из которых следует признать несовместимость систем ЭЦП стран-членов ОСЖД из-за различия в применяемых стандартах, протоколах и технических спецификациях. Как следствие этого, цифровая подпись, наложенная с помощью сертифицированных средств одного государства, не может быть проверена и быть признанной с помощью средств ЭЦП другого государства.

Таким образом, для организации информационного обмена между железными дорогами стран – членов ОСЖД с использованием ЭЦП необходимо решить следующие проблемы:

- создать механизм признания юридического значения подписанного ЭЦП документа и обеспечения доверия сертификатам, изданным в разных правовых полях сторон, и подписать соответствующие нормативно-правовые документы между взаимодействующими сторонами;
- организовать взаимодействие специальных программных и аппаратных средств сторон в правовых полях, определяющих взаимоисключаемость легитимно используемых криптографических алгоритмов;
- организовать технические условия для передачи, обработки и проверки электронных документов, подписанных ЭЦП.

Для признания международного документа во всех странах-участницах ЭДО возникает необходимость наличия в нем подписей на алгоритмах шифрования, признанных в соответствующих странах. Следовательно, каждому участнику ЭДО необходимо иметь две ЭЦП для признания электронного документа как внутри своей страны, так и за ее пределами.

Кроме того, и в России, в странах СНГ юридическая значимость, применимость ЭЦП для удостоверения документов и сделок, определяется законами, нормативными актами и соглашениями сторон.

Таким образом, без решения вопроса об «обмене» криптографическими алгоритмами (либо о выборе «единого» алгоритма обмена), а также без заключения соответствующих соглашений и договоров, как на государственном уровне, так и на уровне взаимодействующих экономических субъектов организация юридически значимого трансграничного электронного взаимодействия не представляется возможной.

7.2. Рекомендации по выбору оптимального варианта организации трансграничного электронного документооборота.

Предлагается вариант построения трансграничного электронного документооборота, который основан на обобщении двусторонних соглашений разных стран по обмену информацией, анализе и обобщении правовых аспектов трансграничного применения электронной подписи с точки зрения законодательства Польской Республики, опыта стран ЕврАзЭС, СНГ, опыта электронной торговли.

Коротко обозначим предметы и уровни правовых отношений, а также характер правовых актов, обеспечивающих права и обязанности каждой из сторон — участников этого процесса. Во-первых, предметом отношений является передаваемый электронный документ или их множество и, во-вторых, объектом правового регулирования являются отношения участников трансграничного обмена.

Эти отношения выглядят следующим образом. Условные субъекты А и Б, каждый из которых имеет свою юрисдикцию, вступают в отношения обмена документами, имеющими юридическую силу: субъект А обеспечивает передачу своего электронного документа путем взаимодействия со своим контрагентом (партнером) Б. Каждый из участников (А и Б) при этом взаимодействует со своей ДТС (ДТС «А» и ДТС «Б»).

Перед ДТС стоят три задачи:

1. Принять корреспонденцию от клиента А, занести в реестр поступивших электронных документов для трансграничной передачи; проконтролировать подтверждение действительности его электронной подписи на момент ее трансляции по системе коммуникаций в зону юрисдикции государства клиента Б.
2. Подтвердить достоверность подписи А другой ДТС (ДТС «Б») путем формирования электронного апостиля, в который включены реквизиты ДТС «А», дата и время его формирования и отправления, удостоверяемые подписью должностного лица ДТС «А», и передать по сети в адрес ДТС «Б» для адресата А.
3. Сообщить клиенту А о произведенных операциях с его ЭД, отослав ему подтверждение (квитанцию), если это предусмотрено договором.

ДТС участников А и Б (ДТС «А» и ДТС «Б») принимают электронные документы или сообщения и фиксируют в своих реестрах факт поступления, контроля электронной подписи, ее заверения (формирования апостиля) и отправки.

7.3. Определение перечня организационно-правовых документов, обеспечивающих осуществление трансграничного электронного документооборота.

Правовое оформление взаимодействия участников информационного трансграничного обмена предполагает заключение соответствующих договоров. В данном случае требуются договоры двух видов: каждого из пользователей услугами ДТС со своей ДТС, а также каждой ДТС со своим зарубежным аналогом (в нашем примере — между ДТС «А» и ДТС «Б»).

Однако этого недостаточно для полноценного правового информационного взаимодействия участников А и Б, которые могут представлять как физических и юридических лиц, так и органы государственной власти разных государств. Необходимы исходные международные акты, регламентирующие порядок реализации трансграничного информационного обмена.

Самое широкое информационное пространство может быть обеспечено таким актом, как международная конвенция по обеспечению трансграничного взаимодействия на основе электронного документа (сообщения) и электронной подписи. Государства — участники такой конвенции, ратифицируя ее, приняли бы на себя обязанности по созданию инфраструктуры и адекватной правовой основы в структуре национального законодательства. Для перехода от конвенции к конкретным

договорам между операторами взаимодействующих государств требуется еще один международный документ — типовой договор операторов стран — участниц конвенции.

На рисунке 11 показано взаимодействие и системная связь правовых актов, обеспечивающих предоставление услуг по признанию легальности электронной подписи в трансграничном информационном взаимодействии субъектов двух или более государств.

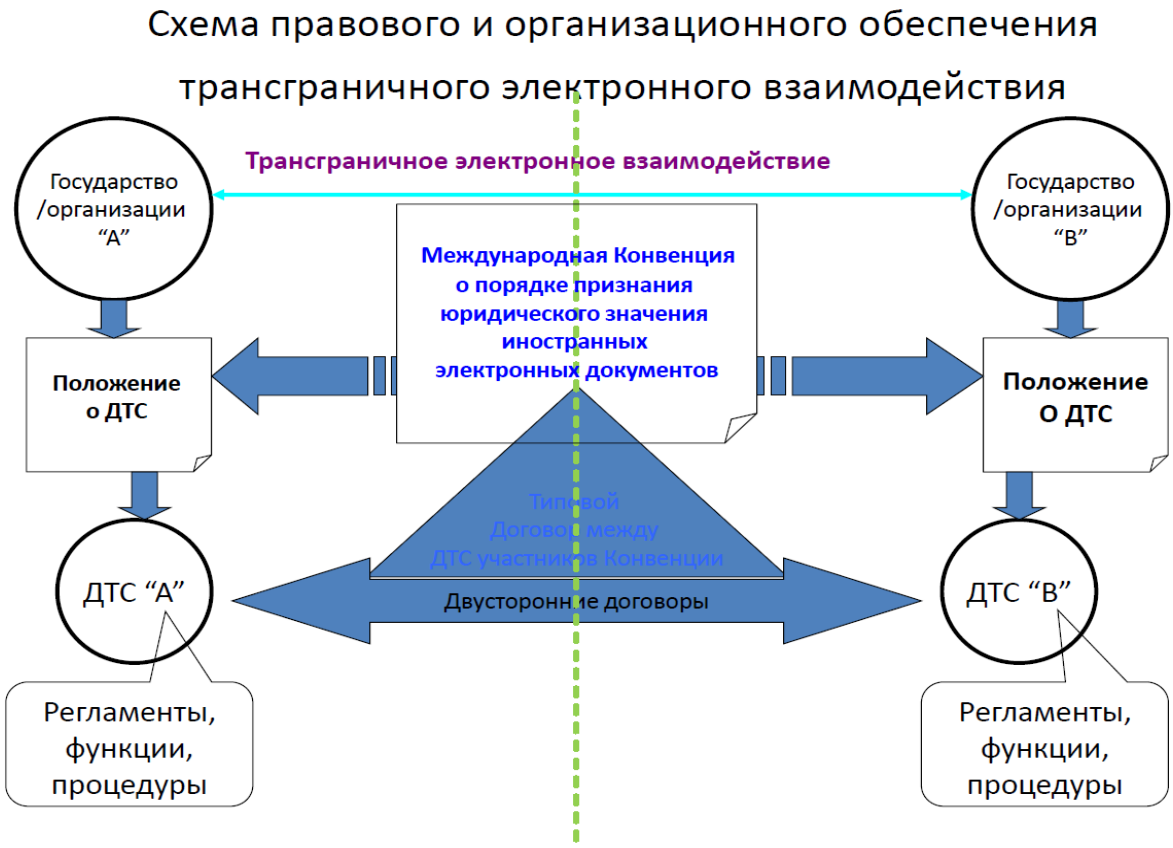


Рис.11. Схема правового и организационного обеспечения трансграничного э. в.

Все виды правовых документов, обеспечивающих процесс трансграничного информационного обмена на основе электронной подписи (электронной цифровой подписи), должны быть предписаны предлагаемой конвенцией и сопровождаться Положениями о соответствующей службе ДТС каждого участника конвенции, определяющими функции, операции, наличие необходимых с точки зрения национального законодательства административных и технических регламентов.

В процессе и этой подготовительной работы предстоит решить ряд проблем. Во-первых, сообщество должно выработать единое мнение об уровне конвенции и порядке ее принятия. Думается, что необходим орган, правомочный принять акт, действующий на наиболее широком информационном пространстве. Во-вторых, важно определить полномочия служб трансграничного доверия, а также их ответственность. В-третьих, важно установить предмет контрольной деятельности оператора — только ли электронная подпись, или это также контент документа.

Кроме того, необходимо закрепить правило, по которому оператор не может притязать на право собственности на реестры, которые он ведет, и на документы,

обращение которых по сети он обеспечивает, однако он отвечает за их неприкосновенность и сохранность, а также конфиденциальность всей информации своей службы.

Для каждой страны — участницы предлагаемой конвенции важно решить вопрос об организационной форме служб ДТС, который бы оперативно мог взаимодействовать со своими удостоверяющими центрами, подтверждающими действенность сертификата на ключи подписи на момент поступления электронного документа в правовое поле контрагента. Он несет ответственность за достоверность и своевременность предоставляемых данных другой стороне трансграничного механизма для определенного адресата на условиях договора между двумя конкретными службами ДТС.

Предлагаемая модель позволит увязать особенности национального законодательства участников конвенции с общими требованиями к обеспечению трансграничного обмена электронными документами и сообщениями.

7.4. Технические и организационные требования к организации работы комплексов ДТС.

В части стандартизации должны быть унифицированы требования взаимодействия ДТС между собой, т.е. определен интерфейс и формат взаимодействия, для того, чтобы субъекты одного ДТС могли надежно связываться с субъектами другой ДТС возможности, а также создать взаимоувязанную сеть ДТС. В случае взаимодействия ДТС и пользователя должны быть установлены единые требования запроса услуг ДТС и предоставления данных для проверки, а также форматы результатов проверки, получаемые пользователем. В отношении криптографических средств формирования и проверки электронной цифровой подписи необходимо установить, на сколько процессы проверки подписи, осуществляемые средством электронной цифровой подписи и ДТС, будут взаимосвязаны, или эти процессы останутся независимыми, сохраняя приоритет проверки ДТС.

В отношении ДТС требуется выработать соответствующую политику безопасности, охватывающую все аспекты безопасности, связанные с управлением ДТС и процессами обслуживания. Должна быть определена и четко разграничена ответственность между ДТС и пользователями услуг ДТС. Обязательства и ответственность ДТС должны быть совместимы с ее финансовой способностью. Пример Типового соглашения между ДТС приведен в приложении 1. В качестве основы, определяющей разграничение ответственности между ДТС и пользователями, может быть использован типовой договор на предоставление услуг Удостоверяющего центра.

Необходимым условием дальнейшего развития сервисов ДТС является разработка гармонизированной методологической базы и поддерживающего её инструментария, позволяющих:

- оценить готовность и совместимость различных информационных систем взаимодействующих сторон к взаимодействию с сервисами ДТС;
- оценить качество и доступность сервисов ДТС.

Ссылки

[1] «trict.tomsk.gov.ru›core/download?objectURI=597,» [В Интернете].

[2] «http://tools.ietf.org/html/rfc3447,» [В Интернете].

[3] «http://tools.ietf.org/html/rfc2560,» [В Интернете].

[4] «http://tools.ietf.org/html/rfc6960,» [В Интернете].

[5] «http://tools.ietf.org/html/rfc2315,» [В Интернете].

[6] «http://tools.ietf.org/html/rfc2630,» [В Интернете].

[7] «http://tools.ietf.org/html/rfc5652,» [В Интернете].

[8] «http://tools.ietf.org/html/rfc2510,» [В Интернете].

[9] «http://tools.ietf.org/html/rfc4210,» [В Интернете].

[10] «http://tools.ietf.org/html/rfc6712,» [В Интернете].

[11] «http://tools.ietf.org/html/rfc5246,» [В Интернете].

[12] «http://www.ietf.org/rfc/rfc4634,» [В Интернете].

[13] «http://tools.ietf.org/html/rfc5280,» [В Интернете].

[14] «http://tools.ietf.org/html/rfc6818,» [В Интернете].

[15] «http://www.rfc-editor.org/rfc/rfc3029.txt,» [В Интернете].

[16] «http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf,» [В Интернете].

[17] «http://www.w3.org/TR/xkms2/,» [В Интернете].

[18] «http://www.etsi.org/deliver/etsi_ts/102200_102299/102231/03.01.02_60/ts_102231v030102p.pdf,» [В Интернете].

Приложение 1

Соглашение о взаимодействии служб ДТС при организации взаимного признания электронных подписей в трансграничном электронном документообороте

Служба доверенной третьей стороны открытого акционерного общества «Российские железные дороги» в лице _____, действующего на основании Положения (Устава), далее именуемая ДТС-А, и Служба доверенной третьей стороны_____ в лице _____, действующего на основании Положения (Устава), далее именуемая ДТС-Б, вместе именуемые «Стороны», заключили настоящее Соглашение о нижеследующем:

1. ПРЕДМЕТ СОГЛАШЕНИЯ

Предметом настоящего Соглашения является:

1.1. Порядок взаимодействия Сторон Соглашения и условия обмена информацией между Сторонами для признания юридического значения иностранных электронных документов и их подписей при международном трансграничном информационном обмене.

1.2. Обеспечение гарантий доверия к электронным документам, удостоверенным Стороной, в юрисдикции которого находится адресат, и признания правомерности применения электронных подписей в исходящих и/или входящих электронных документах в соответствии с правилами и требованиями национального законодательства страны пребывания службы доверенной третьей стороны.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Для целей настоящего Соглашения Стороны используют следующие термины и определения:

2.1. Адресат электронного документа - лицо, которое, согласно намерению составителя электронного документа, должно получить данный подписанный электронный документ, за исключением лиц, действующих в качестве доверенной третьей стороны или иных операторов - посредников в отношении этого электронного документа.

2.2. Составитель электронного документа - лицо, которое или от имени которого электронный документ был подготовлен, подписан и/или отправлен до хранения, если таковое имело место, за исключением лиц, действующих в качестве доверенной третьей стороны или иных операторов-посредников в отношении этого электронного документа.

2.3. Система ЮЗЭДО (юридически значимого электронного документооборота) – информационные системы Сторон, в которых предусмотрен обмен ЭД с использованием ЭЦП и в которой действия участников регламентируются отдельными соглашениями и договорами.

2.4. Служба доверенной третьей стороны (ДТС) – организация, наделенная правом в соответствии с законодательством государства каждой из Сторон или в соответствии с соглашением Сторон осуществлять деятельность по проверке

электронной подписи в электронных документах в фиксированный момент времени в отношении составителя и/или адресата электронного документа.

2.5. Электронный документ – формализованная запись информации в электронном виде, заверенная электронной подписью и отвечающая правилам и требованиям документирования, установленным Сторонами.

2.6. Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

3. ПРАВА И ОБЯЗАННОСТИ СТОРОН

3.1. Настоящее Соглашение в силу равнозначности прав и обязательств Сторон по отношению друг к другу является безвозмездным.

3.2. Стороны обязуются соблюдать порядок обмена документами в соответствии с условиями, установленными настоящим Соглашением.

3.3. Каждая Сторона по настоящему Соглашению действует и ведет финансово-хозяйственную деятельность в рамках своего национального законодательства и установленных полномочий.

3.4. В части стандартизации должны быть унифицированы требования взаимодействия ДТС между собой, т.е. определен интерфейс и формат взаимодействия, для того, чтобы субъекты одного ДТС могли надежно связываться с субъектами другой ДТС возможности, а также создать взаимоувязанную сеть ДТС. В случае взаимодействия ДТС и пользователя должны быть установлены единые требования запроса услуг ДТС и предоставления данных для проверки, а также форматы результатов проверки, получаемые пользователем.

3.5. Стороны имеют право:

3.5.1. Передавать информацию, связанную с оказанием услуг доверенной третьей стороны по запросам уполномоченных на то лиц и организаций, имеющих право на их получение в порядке и в соответствии с действующим законодательством Сторон.

3.5.2. Приостанавливать информационный обмен на условиях и в порядке, установленном техническими регламентами по проведению регламентных и профилактических работ.

3.5.3. Помимо услуг, указанных в п. 3.6.12 настоящего Соглашения, оказывать иные дополнительные услуги, связанные с организацией юридически значимого электронного документооборота.

3.6. Основными взаимными обязательствами Сторон по настоящему Соглашению по отношению друг к другу являются:

3.6.1. Обеспечение в трансграничном обмене взаимных гарантий и доверия к электронным документам, обеспечение правомерности применения электронных подписей и способов защиты исходящих и/или входящих электронных документов в соответствии с правилами и требованиями национального законодательства страны пребывания Стороны настоящего Соглашения.

3.6.2. Обеспечение в соответствии с требованиями национального законодательства каждой из Сторон настоящего Соглашения другой Стороны (на условиях взаимного обмена) необходимыми регламентами и программными средствами (интерфейсом) для проведения проверок электронных документов и/или их электронных подписей, исходящих от другой Стороны.

3.6.3. Автоматизированное заверение или удостоверение с формированием электронной квитанции электронных документов своей Стороны и/или их электронных подписей по запросам другой Стороны.

3.6.4. Легализация Стороной настоящего Соглашения на основе проведения автоматизированной процедуры проверки всех получаемых от другой Стороны транзитных электронных документов и их соответствующих им квитанций, сформированных другой Стороной, путем заверения или удостоверения в соответствии с требованиями национального законодательства Стороны, в которой электронный документ или сообщение должны быть использованы адресатом.

3.6.5. Экспертиза и проверка электронных подписей в электронных документах на подлинность и соответствие требованиям национального законодательства страны с выдачей экспертных заключений в порядке, установленном законодательством страны пребывания Стороны.

3.6.6. Каждая Сторона при исполнении процедур заверения или удостоверения электронных документов своей Стороны и/или их электронных подписей обязана сформировать электронную квитанцию и передать ее другой Стороне установленным способом.

3.6.7. Электронная квитанция должна содержать следующие сведения:

- электронную подпись уполномоченного лица службы доверенной третьей стороны, от имени которого проводилась процедура заверения или удостоверения электронного документа с указанием его имени, фамилии и должности;
- официальные реквизиты службы доверенной третьей стороны;
- регистрационный номер электронной квитанции, дату и время ее формирования.

3.6.8. Каждая Сторона настоящего Соглашения обязана вести и поддерживать в актуальном и безопасном состоянии электронный реестр (базу данных), в котором должен регистрироваться каждый факт заверения (удостоверения) электронного документа (сообщения) или его электронной подписи и факт формирования электронной квитанции.

3.6.9. В состав сведений электронного реестра должны входить:

- регистрационный номер электронной квитанции;
- дата и время формирования электронной квитанции и регистрационной записи в реестре;
- атрибуты и реквизиты заверяемой (удостоверяемой) формы представления и оборота электронного документа и/или его электронной подписи;
- электронная квитанция с электронной подписью уполномоченного лица службы доверенной третьей стороны, от имени которого проводилась процедура заверения или удостоверения электронного документа, его имя, фамилия и должность;

- иные дополнительные сведения (например, сведения о подтверждении факта получения электронного документа адресатом).

3.6.10. Каждая Сторона обязана вести автоматизированное документирование всех своих действий и процессов, происходящих в системе ЮЗЭДО Стороны и связанных с исполнением услуг ДТС с пошаговой фиксацией даты и времени;

3.6.11. Каждая Сторона по запросам другой Стороны обязана провести экспертизу электронной подписи в электронных документах, сформированных в ее юрисдикции, и предоставить другой Стороне экспертное заключение.

3.6.12. Каждая Сторона обязана обеспечивать другую Сторону по ее запросам доказательствами, связанными с действиями Стороны по фактам оказания услуг:

- по подтверждению фактов отправки отправителем и/или получения адресатом электронных документов;
- по фактам заверения или удостоверения электронных документов;
- по фактам удостоверения электронных подписей;
- по экспертизе (проверке) электронных подписей в документах;
- по архивированию и депозитарному хранению контрольных экземпляров электронных документов;
- по исполнению иных действий, связанных с оказанием услуг службы ДТС.

3.6.13. Стороны обязуются в процессах оказания услуг выполнять требования по обеспечению информационной безопасности и конфиденциальности информации, содержащейся в транзитных документах и сообщениях, в соответствии с международными рекомендациями и требованиями действующего законодательства Стороны.

3.6.14. Каждая Сторона по настоящему Соглашению обязана иметь необходимые лицензии, сертификаты или аттестацию на ведение деятельности по оказание услуг третьей доверенной стороны, если в соответствии с требованиями действующего национального законодательства таковые необходимы.

4. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ

4.1. Стороны самостоятельно организуют взаимодействие со своими системами ЮЗЭДО, участвующими в трансграничном информационном обмене. При этом Стороны не несут ответственность за прямое взаимодействие систем ЮЗЭДО, если такое взаимодействие предусмотрено порядком организации трансграничного информационного обмена.

4.2. Стороны договорились о том, что Стороны признают юридическую силу электронных документов исходящих от составителей, подпадающих под юрисдикцию противоположной Стороны и выполненных по правилам и требованиям ее национального законодательства, если электронный документ имеет электронную квитанцию Стороны составителя, оформленную в соответствии с требованиями международных рекомендаций ITU-T X.842 «Информационная технология – методы безопасности - Руководящие принципы для использования и управления услугами доверенной третьей стороны».

4.3. Стороны для организации информационного взаимодействия используют следующие протоколы обмена информацией и унифицированные форматы представления данных:

- RFC 3029. Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (DVCS).
- RFC 2560. Online Certificate Status Protocol - OCSP.
- RFC 3161. Time-Stamp Protocol (TSP).

4.4. Электронные документы для прохождения процедуры легализации направляются заинтересованными пользователями Стороне настоящего Соглашения, в юрисдикции которой они находятся с указанием электронного адреса конечного адресата.

4.5. Легализация Сторонами электронных документов и их электронных подписей при трансграничном информационном обмене, а также порядок технического и технологического сопряжения служб ДТС Сторон устанавливаются на основе согласованного Сторонами регламента взаимодействия (Приложение 1 к настоящему Соглашению).

4.6. Стороны заверяют или удостоверяют целостность и подлинность электронных документов и/или соответствие их электронных подписей правилам и требованиям национального законодательства, если иное не установлено межгосударственным соглашением.

4.7. Стороны не заверяют или не удостоверяют соответствие содержания (контента) электронных документов сообщений требованиям национального законодательства, если иное не установлено межгосударственным соглашением или национальным законодательством.

4.8. Стороны признают, что используемые Сторонами средства защиты информации обеспечивают достаточную защиту и целостность электронных документов и позволяют идентифицировать лиц, от имени которых используется электронные подписи в порядке, установленном правилами и требованиями законодательства каждой Стороны.

5. ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. Стороны за ненадлежащее исполнение своих обязательств по настоящему Соглашению несут материальную ответственность в соответствии с требованиями национального законодательства.

5.2. При передаче документов и сообщений, полученной от третьих лиц, Стороны отвечают за точность и своевременность её обработки, за целостность и соответствие данных полученного и передаваемого сообщения, соблюдение требований обеспечения конфиденциальности информации. Стороны не несут ответственности за содержание (контент) транзитных электронных документов и/или сообщений, если иное неустановленное межгосударственным соглашением или национальным законодательством.

5.3. Каждая Сторона отвечает за все действия, совершаемые лицами, которые уполномочены этой Стороной выполнять от ее имени установленные процедуры и/или

услуги доверенной третьей стороны в процессах легализации электронных документов и их электронных подписей.

6. ПОРЯДОК РАССМОТРЕНИЯ СПОРОВ

6.1. Стороны обязуются соблюдать претензионный порядок урегулирования споров и разногласий, возникающих из настоящего Соглашения.

6.2. Право предъявления претензий принадлежит отправителю или получателю электронных документов (далее – заявитель). Претензии должны быть предъявлены заявителем к Стороне настоящего Соглашения, соответствующей стране его пребывания.

6.3. Претензия заявляется Стороной, получившей ее от заявителя, другой Стороне (Сторона-ответчик) в письменной форме и должна быть подписана уполномоченным представителем Стороны, заявляющей претензию. Претензия должна содержать:

- изложение требований заявителя;
- изложение обстоятельств, на которых основываются требования заявителя, и доказательства, подтверждающие их, со ссылкой на соответствующее законодательство;
- перечень прилагаемых к претензии документов и других доказательств;
- иные сведения, необходимые для урегулирования спора.

6.4. Претензия рассматривается Стороной-ответчиком в течение _____ дней со дня ее получения. Если по претензии потребуются дополнительные документы, необходимые для ее рассмотрения, они запрашиваются у Стороны-заявителя претензии. При этом указывается срок, необходимый для их представления. В случае неполучения затребованных документов к указанному сроку, претензия рассматривается на основании имеющихся документов.

6.5. Ответ на претензию представляется Стороне-заявителю, подписывается уполномоченным представителем Стороны-ответчика. Непредставление ответа на претензию в течение _____ дней с даты получения претензии рассматривается как отказ в удовлетворении претензии.

6.6. Споры между Сторонами, связанные с толкованием и (или) применением положений настоящего Соглашения, разрешаются, в первую очередь, путем проведения переговоров и консультаций.

6.7. Если спор не будет урегулирован Сторонами путем переговоров и консультаций в течение шести месяцев с даты официальной письменной просьбы об их проведении, направленной одной из Сторон другой Стороне, то, при отсутствии иной договоренности между Сторонами относительно способа его разрешения, любая из Сторон может передать этот спор для рассмотрения в надлежащем суде той страны, железным дорогам которой была предъявлена претензия.

7. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ

7.1. Стороны освобождаются от ответственности за частичное или полное неисполнение своих обязательств по настоящему Соглашению, если это неисполнение

явилось следствием обстоятельств непреодолимой силы, возникших после заключения настоящего Соглашения, или в результате событий чрезвычайного характера, а также сбоев, неисправностей и отказов оборудования; сбоев и ошибок программного обеспечения; сбоев, неисправностей и отказов систем связи, энергоснабжения, кондиционирования и других систем жизнеобеспечения, не позволяющих осуществлять эксплуатацию необходимого для выполнения настоящего Соглашения оборудования, которые Стороны не могли предвидеть или предотвратить.

7.2. В случае возникновения обстоятельств непреодолимой силы срок выполнения Сторонами своих обязательств по настоящему Соглашению отодвигается соразмерно времени, в течение которого действуют такие обстоятельства и их последствия.

7.3. Сторона, для которой стало невозможным выполнение своих обязательств в виду действия обстоятельств непреодолимой силы, обязана немедленно сообщить другой Стороне о начале, изменении масштаба, характера и прекращении действия обстоятельств, воспрепятствовавших выполнению договорных обязательств.

7.4. Обязанность доказывать существование обстоятельств непреодолимой силы лежит на Стороне, которая ссылается на их действие.

7.5. По прошествии обстоятельств непреодолимой силы Стороны обязуются принять все меры для ликвидации последствий и уменьшения причиненного ущерба.

8. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ

8.1. Настоящее Соглашение вступает в силу с момента его подписания Сторонами и действует до _____. Дата начала обмена Сторонами электронными документами в соответствии с условиями настоящего Соглашения определяется датой, установленной нормативными документами (распоряжениями) руководящих органов Сторон о начале обмена электронными документами с электронной подписью.

8.2. Соглашение считается продленным на каждый последующий календарный год, если ни одна из Сторон за 1 (один) месяц до истечения указанного срока не представила другой Стороне письменное заявление о намерении расторгнуть настоящее Соглашение.

9. УСЛОВИЯ РАСТОРЖЕНИЯ

9.1. Каждая из Сторон вправе расторгнуть настоящее Соглашение, письменно уведомив другую Сторону за _____ дней. Соглашение считается расторгнутым по истечении _____ дней со дня направления такого уведомления.

10. УСЛОВИЯ КОНФИДЕНЦИАЛЬНОСТИ

10.1. Информация, содержащаяся в электронных документах, является конфиденциальной, если иное не установлено ее обладателем, и не подлежит

разглашению третьим лицам. Стороны обязуются сохранять конфиденциальность этой информации и не раскрывать ее третьим лицам.

11. ПРОЧИЕ УСЛОВИЯ

11.1. Любые договоренности Сторон относительно взаимоотношений, регулируемых настоящим Соглашением, влекущие за собой необходимость внесения изменений в настоящее Соглашение, должны быть письменно подтверждены Сторонами путем подписания дополнительного соглашения.

11.2. В случае принятия международных или межгосударственных соглашений или иных нормативных правовых актов по вопросам, регулируемым настоящим Соглашением, изменение соответствующих положений настоящего Соглашения оформляется дополнительным соглашением, которое должно быть заключено в течение 30 дней со дня вступления указанных актов в силу.

11.3. Изменения и дополнения в настоящее Соглашение могут быть внесены по дополнительному соглашению Сторон, оформленному в письменном виде и подписанному полномочными представителями Сторон.

12. ПРИЛОЖЕНИЯ К СОГЛАШЕНИЮ

(разрабатываются взаимодействующими сторонами дополнительно)

Приложение № 1: Регламент взаимодействия Служб ДТС при эксплуатации комплексов программно-технических средств при организации взаимного признания электронных подписей в трансграничном электронном документообороте.